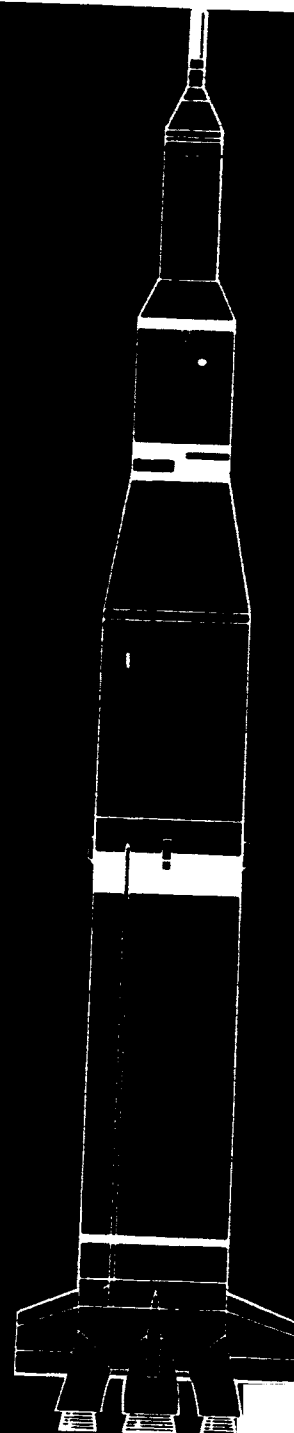# SYRACUSE / NASA
PROGRAM

NASA National Aeronautics and
Space Administration

Syracuse University

MANAGEMENT OF SAFETY AT NASA

by

Martin E. Barzelay
Rajan Chandran
John E. LaGraff
David L. Wilemon
Bernard D. Wood

6223-R-3

SYRACUSE/NASA PROGRAM

Grant No. NGL 33-022-090

MULTIDISCIPLINARY STUDIES IN MANAGEMENT AND
DEVELOPMENT PROGRAMS IN THE PUBLIC SECTOR

Prof. Martin E. Barzelay
Principal Investigator

SYRACUSE UNIVERSITY

Syracuse, N. Y.

August 1974

CONTENTS

I. SUMMARY

NASA's organizational arrangement for the management of safety and safety-related functions varies from Center to Center and from program to program, depending on the history and mission of each. While this has resulted in a diversity of safety management, the Safety and Reliability and Quality Assurance office at NASA Headquarters has been a unifying influence. Safety, Reliability and Quality, all assurance functions, have become intertwined in all programs but often at different levels. Thus, while it is strongly indicated that any safety office should occupy a commanding and prominent position, not all do. It appears that the more that Safety (like Reliability and Quality Assurance) is institutionalized, the greater will be the continuity of project safety. This is especially true since the response to any safety request or directive depends for its effectuation not only on the source but also on the actual or perceived authority of that source. It should be obvious that as safety is institutionalized the key positions should be staffed by personnel with test, operational and design experience.

The fact that NASA is a project-oriented Agency makes it difficult for a continuing function such as Safety Assurance to achieve stability and continuity within any given project. However, we found that while a specific Systems Safety office could not be found in certain Centers or in certain programs, this did not mean that systems safety work was not being carried out. The argument was presented by many within NASA that good engineers and good management automatically take care of safety

and the program manager is responsible for safety assurance. We feel, however, that the institutionalization of Safety, suggested above, is also desirable because: a) NASA's programs are too complex for a given project or program to be isolated from others, and b) NASA no longer has the funds or manpower it had in the past to duplicate efforts. Only through centralized SR&QA offices can the past efforts be applied by the most knowledgeable individuals on all projects.

It is our conclusion that the key to safety assurance lies in a systematic approach to hazard identification and analysis and that this is best provided by a safety office. It should be especially noted that where a safety condition is recurrent it can be looked at in terms of the overall system and from a broader experience base by such an office. Further, and even more important, early penetration of a project from the conception stage is essential for effective safety input. Assuming an early penetration, the three key stages at which safety input is more effective are: 1) Requests for Proposals, 2) Source Evaluation Boards, and 3) Change Control Boards. Unfortunately, getting Systems Safety studies into a program as early as possible are even now far from automatic. As a recent example, Systems Safety studies were minimal in the early stages of the Shuttle program, necessitating compromises in Phases C and D that might otherwise have been avoided.

Experience retention and dissemination are absolutely necessary for an effective safety program. As examples, the Johnson Spacecraft Center has prepared the "Apollo Experience Papers," and a set of design

standards have been developed from lessons learned on past programs. It would appear particularly appropriate for the Aerospace Safety Research and Data Institute at the Lewis Research Center to compile accident/incident histories, as at JSC, for NASA-wide dissemination.

Headquarters

Centralized responsibility for assurance functions is placed in the Safety and Reliability and Quality Assurance Office (SR&QA at Headquarters). This location is considered logical and sufficiently high in the NASA organization. Despite this position, there appears to be a less than desirable influence on relevant offices at the Office of Manned Space Flight Centers, since OMSF has its own RQ&S office. There appeared to be a better organizational compatability and unity of purpose between Headquarters and JSC than between Headquarters and other Centers, probably due to a history of personal contact with SR&QA.

An entirely independent safety organization at Headquarters is the Aerospace Safety Advisory Panel (ASAP), which was set up directly by Congress. This Panel, which reports directly to the NASA Administrator and his Deputy, provides a special overview of management operations as they affect reliability in general, and critiques important safety-related incidents. "Safety" in the title is too narrow since the Panel is also concerned with technical and administrative management and is in essence a management advisory group. While ASAP is not a regulatory agency and has no line responsibility or authority, it carries considerable weight since it reports to the NASA Administrator and to the Congress.

We found very little direct contact between ASAP and the SR&QA office at Headquarters. In our opinion, more frequent contact, formal or otherwise, would be valuable to both.

Johnson Space Center

Of all the Centers visited in this study, JSC appeared to have the most effective SR&QA office. There appear to be several reasons for this: 1) their involvement with Manned Spacecraft, 2) the relationship established by the present director of SR&QA, who was at one time at Headquarters, and 3) the managerial handling of the Operations Safety branch in such a way as not to dilute program and mission safety with institutional safety (although it is not in any way implied that this has been neglected). Evidence of the effectiveness of SR&QA at JSC was most apparent in the close ties with programs and with the E & D directorate. The director of SR&QA had three Special Assistants in his office, one each for Apollo, Skylab, and Space Shuttle, who were at the same time Special Assistants to the three respective program directors, with their appointments approved by both the director of SR&QA and the program manager in each case. While these Special Assistants do not have direct authority and are primarily liaison men, they are staff members in their respective program offices, at the top of the program at the Center, thus having a high degree of perceived authority. Further, at JSC, while E & D does not in itself have a safety office, SR&QA personnel were assigned to each subsystem project office in E & D. An important but seemingly obvious device at JSC to

facilitate communication among groups with overlapping assurance respon-
sibilities was to locate them close together in the same building. While
seemingly minor, the juxtaposition of related offices encourages mutual
support and, in our opinion, is an important contributing factor to the
encouragment of safety cooperation.

Marshall Space Flight Center

The office responsible for safety at the Marshall Space Flight
Center is called Safety and Manned Flight Awareness. As one of several
staff level offices it is basically in the same position in the Center
organization as SR&QA at JSC, but a major difference between the two is
indicated by the title of the office; at MSFC the office has no direct
responsibility for reliability and quality assurance, and there is no
staff level office for R & QA. However, MSFC was the only Center which
had a Manned Flight Awareness office with NASA-wide responsibility for
manned programs. We feel that MSFC's management of safety-related
assurances was strongly influenced by the history of the Center. The
Laboratories in the Science and Engineering directorate were always
strong and there was no direct connection between S & MFA and Quality
and Reliability Assurance, which remained in the Laboratories. While
there seemed to be a close working relationship at MSFC between the
director of S & MFA and the deputy director of Systems/Products in
S & E, the relationship was not structured by formal sign-off authority.
Similarly, there was no sign-off authority granted to a Safety or Q & RA

man in projects or programs. Neither were there Safety men co-located
in program offices. We consider this lack of sign-off authority to be
of considerable importance because the S & FMA office does not have
sufficient strength to penetrate the major activities of the Center.

Goddard Space Flight Center

At the Goddard Space Flight Center the office of Health and Safety
Engineering (H & SE) is nominally responsible for institutional plant
safety and project system safety. The Health section is mainly devoted
to environmental and plant safety, while the primary function of the
Safety section is the encouragement of a systems safety plan for each
new project. Requirements for this plan are formalized in a Goddard
Management Instruction, which also requires the appointment of a proj-
ect Safety Officer. While compliance with the general provisions of
the manual are supposedly assured by top Center management, it was
apparent that these procedures were not considered absolutely vital
by some engineers and project managers. Some of the managers were in-
clined to view the H & SE office to be concerned with health and indus-
trial safety only, while safety assurance was an integral part of the
project manager's job. The R & QA office, though completely separate
from H & SE, was considered to be only advisory to the project offices.
Goddard has always placed great reliance on testing and well-developed
test procedures. However, with current budget limitations, testing to
the extent that it was done in the past has become too expensive, pri-
marily because it comes relatively late in the development of a system.

While there is a system engineer on each project, the establishment of a formal system safety review procedure has been resisted. There appears to be a strong feeling that the goal must be adequate performance at low cost and that NASA must be prepared to accept more risk in unmanned than in manned missions, and the one way of achieving lowered costs is by saving the cost of systems safety analysis. However, in the final analysis, Goddard has not been as averse to system safety studies as appears on the surface. They have, in fact, obtained assistance from Headquarters SR&QA for detailed studies on specific problems and have carried out systems safety studies by testing and other procedures while not calling them by that name. In our view, safety assurance should be involved in projects and programs from their inception and the concerned safety office should be highly placed in the management structure. In short, Goddard is better than it looks on the surface, but there is room for improvement.

Lewis Research Center

At the Lewis Research Center the committee and panel structure which has evolved is probably appropriate for a research-oriented operation like Lewis. Such Centers are concerned with diverse experimental programs and with major test facilities and not with the programmatic safety problems of the Office of Manned Space Flight.

Coordination of activities between the various committees and panels is provided by the Executive Safety Board. That Board's Executive Secretary

is also the Lewis Safety Officer and as such is also an ex-officio member of each Area Safety Committee. This multiple role provides coordination, but also creates uncertainty for some laboratory-level staff. Such ambiguity is potentially a detriment to safety operations. The difficulty of deciding the importance of and attending Area Safety Committee meetings with limited staff is also a problem for the Safety Officer.

The lack of formal relationships between the various Lewis Safety Committees and Panels is of concern. It appears that the integration and coordination of the various Committees' efforts is primarily accomplished through the interpersonal relationships of the members. We question whether this is good management policy. Formal relationships and policies could help insure the continuity and completeness of a committee's efforts.

We also have been concerned about the real role of the Project Planning and Safety Office. The question we raise is whether this Office is truly involved in the planning of safety for projects, or simply performs the role of expeditor in procurement, etc. Our interviews revealed that there were some conflicting opinions on the extent of this Office's safety role in project planning.

A final point which should be raised is the extent of the decentralized activities of the Lewis Safety and Project Planning Office. Too much decentralization can waste both human and materiel resources. We question whether all the separate activities which have been grouped under the Safety and Project Planning Offices do require the separate,

small organizational units. A close examination of the functions each
"office" performs might reveal that a consolidation of these activities
is needed and would promote efficiency.

Aerospace Safety Research & Data Institute

With regard to the Aerospace Safety Research & Data Institute (ASRDI),
at the Lewis Research Center, we found that while safety information trans-
fer is an important and complex process, it has not been optimally carried
out by ASRDI. Divergent points of interpretation or perceptions of
ASRDI's charter, research versus information transfer, should be resolved.
It is our belief that the prime barriers to a more effective functioning
of ASRDI are:

    a. Conflicts in priorities

    b. Lack of visibility

    c. Staffing inadequacies

The present staff is more research oriented than information transfer
oriented. To help the transfer process we have suggested the use of
Safety Application Teams along the lines of NASA's Biomedical & Tech-
nology Application Teams. We also feel that ASRDI should take the
initiative in the transfer function. Since organizational structures
and practices do affect the transfer process, more formalized contact
points and shifting ASRDI out of Lewis' control may be beneficial. A
survey of users' needs has to be undertaken and plans made to meet these
needs.

II. INTRODUCTION

As part of the ongoing grant from NASA entitled "Multidisciplinary Studies in Management and Development Programs in the Public Sector," the work which had continued since 1968 on various aspects of NASA management methods was extended by the present research into the area of Management of Safety at NASA. Since it is well recognized that the efficient utilization of safety information is both a management and an engineering problem it was considered that an interdisciplinary effort similar to that utilized in previous management studies under the Syracuse/NASA Program could effectively bring together the combined expertise to make a meaningful study of Safety Management at NASA.

It was the purpose of this study to undertake an analysis of both the engineering and management approaches to safety in a complex technological program with many interfaces. Existing practices at various Centers and at Headquarters were examined to determine the organizational areas for the establishment of prime responsibility for Safety. To accomplish this, comparisons were made of the application of safety management techniques between manned and unmanned programs, between one Center and another, and between one program and another. At attempt was made to determine the ultimate responsibility for safety and the effectiveness of this effort.

In the examination of NASA's safety practices the roles of various interface mechanisms were examined. These interfaces exist between organizational entities, formally set up for various purposes, such as the Configuration Management Board, the various Review Boards, the Inter-Center

Panels, the Management Council and the Aerospace Safety Advisory Panel.

The study examined topics as diverse as NASA's attempt to integrate System Safety activities as an integral part of every program rather than treating them as add-on activities, and management aspects of the Aerospace Safety Research and Data Institute (ASRDI) at the Lewis Research Center. The findings regarding ASRDI are included as Chapter IV of this report.

For those unfamiliar with safety terminology and Systems Safety terminology in particular, Appendix A, presenting the terminology of safety, Systems Safety, risk and related factors has been provided. It is suggested that the reader, whether he is familiar or unfamiliar with the terminology, spend a few minutes with this Appendix to familiarize himself with the words as we have used them in the main body of the report. In addition to terminology we have also provided the elements of what we consider to be the essentials of a Systems Safety program. Parts of Chapter III have utilized these elements as a frame of reference.

With regard to methodology, the key research staff who carried out this study had already had considerable success in obtaining information through direct interviews with managers and other personnel within NASA. It was therefore decided to carry out the major part of this investigation in the same manner through direct interviews with personnel in key positions who could discuss actual practice within the Agency. Wherever possible contacts already made by the Syracuse/NASA Program project management study group were made use of. Thus considerable value was derived by the credibility and trust relationships which had been established

over a considerable period of time. Additionally, use was made of documents furnished by the key NASA personnel who were interviewed.

In acquiring information for this report only a limited number of selected offices could be visited due to limitations of time and funding; thus the selection was somewhat arbitrary. However, the conclusions drawn were reached only after members of the research group were confident that the various points made were substantiated and confirmed by remarks or answers to direct questions by NASA personnel, and by our own comparisons of the different offices and their differing modes of operation. Our contacts at the Goddard Space Flight Center were fewer and briefer than at the other Centers reported on herein. Therefore, our comments regarding Goddard are not as extensive as those regarding the other Centers.

In carrying out the work of the project we wish to acknowledge the more than considerable help and interest of Mr. Charles W. Childs, Safety Division, Office of Safety and Reliability and Quality Assurance; and Mr. Jerome D. Morris of the Office of University Affairs, NASA Headquarters. In addition, Mr. Frank Belles, Director of the Aerospace Safety Research and Data Institute, Lewis Research Center; Mr. Martin L. Raines, Director of Safety and Reliability and Quality Assurance at JSC; and Dr. Leslie W. Ball, Director of Safety and Manned Flight Awareness at MSFC, were particularly helpful. Finally, we wish to give credit to Mrs. Jean T. Golemo, Program Manager, who held us all together within the University organization.

III. MANAGEMENT OF SAFETY AT NASA

A. INTRODUCTION

NASA's organizational arrangement for the management of safety and related functions varies from one Center to another and from one program to another, depending on the history and mission of each. Despite this diversity, there has been a serious attempt to coordinate and track these activities as much as possible through the Safety and Reliability and Quality Assurance office at NASA Headquarters. Because safety assurance was given much more prominence in all NASA activities after the disastrous AS-204 fire in 1967, many of the safety offices were either newly created or put in more prominent positions organizationally at that time. By then, of course, NASA and its Centers had developed a very complex organizational structure, the ties of each program and each Center to Headquarters having developed differently as affected by the history and particular requirements of the programs and special responsibilities of the individual Centers.

Undoubtedly, the position of a safety office in any Center has depended to a large extent on the Center director, his management style, his willingness to delegate authority, and his perception of safety and the related functions. It also had to depend on the strengths of the individuals who found themselves responsible for these functions and on their credibility in their Centers.

NASA has always allowed authority to be somewhat ambiguous and has depended on an individual's powers of persuasion (which, in turn, depend on what respect he has among his peers) to assure that critical problems

are dealt with effectively once an appropriate forum is provided. This is satisfactory when what is important in the view of Headquarters is also believed to be important to all concerned at all levels. Unfortunately, this is not always true with regard to safety. Any safety office should occupy a commanding and prominent position; not all do.

While no one in NASA denies the importance of safety in all aspects of NASA's work, there is a considerable divergence of views on how safety is to be achieved and whose responsibility it is or should be. The response to any safety request or directive (as for anything else) depends on the source and the actual or perceived authority of that source. Too often "safety" by itself carries very little weight. Part of the reason for this is the prejudice of most design and operating engineers towards plant or industrial safety engineers who are not perceived as being associated with the prime tasks of NASA; this prejudice is of course common in many industries.

By contrast, Reliability Assurance, Quality Assurance and Testing are functions that all NASA engineers and managers are familiar with, and they have come to rely heavily on these offices at all levels and in all Centers. It makes nice rhetoric to say that Safety relates to human engineering problems; Reliability relates to hardware and design; and Quality relates to manufacturing. But there is not a neat one-to-one relationship here because these are not separate problems. Safety, Reliability and Quality are all assurance functions, inextricably intertwined in all programs whether manned-mission oriented or not.

The fact that NASA is a project-oriented agency makes it very difficult for a continuing function such as safety assurance to achieve stability and continuity within the projects themselves. The more that Safety (like Reliability and Quality Assurance) is institutionalized, the greater will be the continuity of project safety. Programs and projects have very specific and predictable life expectancies and must derive their stability from the continuing resources of the institution.

The fact that a "Systems Safety" office cannot be found in certain Centers or on certain programs does not mean that systems safety work is not being done at all in those organizations. In the first place, essentially the same kind of organized analysis is often undertaken in the course of system design and review. Secondly, various projects frequently borrow expertise from the Headquarters SR&QA office or other NASA offices for a particular study; in the larger programs much safety analysis is done under contract by industry.

There is certainly some justification for the argument that good engineering and good project management automatically take care of safety, and that it is the project or program manager's responsibility to include safety assurance in all decisions or "trades". If his job is done properly, he needs no outside organization duplicating his own program control office. He can utilize the conventional R & QA available in his own program and his own Center.

There are, however, two good reasons why that argument is not defensible: First, NASA's programs are too complex for one program or project to be isolated from all others. Each needs the expertise of others in all phases of its development. No project manager can be sure he is

doing a complete job if he ignores other programs or other centers. Second, NASA no longer has the funds or the manpower to duplicate efforts. True, a certain amount of duplication is an accepted way of providing assurance. During the most active period of the Apollo program, while hardware and operational procedures were being developed against a stringent time schedule and with a very limited experience base, it was not only expedient but also advisable to encourage more than one group to work on a new problem and to check and recheck all procedures. NASA is more mature, experienced and confident now. At the same time all budgets are much more restricted than they had been. It is most efficient to have any job done by the most experienced group and to avoid having similar jobs in different projects or at different centers done by isolated groups unaware of each other's successes and failures. Only through centralized SR & QA offices can the best efforts be applied by the most knowledgeable individuals on all projects. There is bound to be over-lapping of concerns and responsibilities with others wherever safety is involved. No safety office has sufficient staff to do its whole job, but by cooperating with and utilizing other offices, such as R & QA and Systems Integration, they can have a major impact. Primarily, the safety office must assure that an organized, systematic approach is taken with regard to potential hazards.

System Safety is still viewed with little enthusiasm by many. An Air Force representative, speaking as a manager, said that system safety is "more trouble than it is worth". He hastened to say that "safety studies are necessary" and must go along with reliability and quality assurance.

Still, his prejudice was obvious. An experienced program manager warned that "safety people tend to be cultists," implying that they will do studies for the sake of the studies rather than for the good of the program and they are not always realistic. His prime complaint was with studies that tell him after the fact what should have been done when that is perfectly clear to him without the study. He would have valued the same information much earlier in the design, manufacturing, and testing phases.

No designer or project manager will knowingly "sign off" on an unsafe design. But the key to safety assurance is a systematic approach to hazard identification and analysis. This is best provided by a safety office. Although that office may not actually have veto power in a program, a program manager will not take lightly a strong objection from Safety.

Early penetration of a project, right from the conception stage, is essential for effective safety input. It is in the development of a new program plan that connection with past experience is vital. Furthermore, of utmost significance in determining the ability of safety personnel to influence programs is their perceived closeness of association with the program in its earliest development stages. It is appreciably more diffi-cult to convince program people of the validity of your criticism if you are viewed as basically an outsider with no intimate knowledge of the process which led to the existing design configuration. This very natural resistance to outside criticism is apparent at all levels of the review process.

If, on the other hand, the personnel responsible for the safety assurance function have been assigned to the program office at all levels of design and in all phases of development, their safety-related criticism

at any point carries much more weight during review sessions. They are much better known by their colleagues and they know the design history of the program.

There are three key stages at which safety personnel must make their input to a program in order to be most effective: 1) Requests for Proposals, 2) Source Evaluation Boards, and 3) Change Control Boards. Of particular importance is the input to the RFP's. The inclusion of such requirements as a Risk Hazard Summary in a request for proposal makes that document a pressure point in the insistence of hazard analysis in a contract. The potential thoroughness of hazard analysis should be evaluated by the Source Evaluation Boards along with all other technical factors in a proposal. Experience shows that the requirement of a project hazard summary does not increase the proposed cost greatly and may save money in the end, particularly in change proposals, because all the elements of a hazard summary must be undertaken eventually in any normal NASA program. The insistence on a summary at the earliest possible time simply assures a systematic, organized approach.

The necessity of getting System Safety studies into a program as early as possible may seem quite obvious now, but the practice is not old and is even now far from automatic. For instance, System Safety studies were minimal in Phase A of the Shuttle program. There was Hazard Analysis in Phase B. The late introduction necessitated many "trade studies," i.e. compromises, in Phases C and D that might otherwise have been avoided.

An obvious advantage in locating Safety people in program offices is the liaison capabilities this provides. The group primarily responsible for the assurance function (SR & QA) is made directly aware of developments in the program offices and does not even have to wait for formal review meetings to make an input. Also, these program-located safety people are able to identify expertise within the Safety office. The existance of such a capability at the Center may not even be known to other program engineers, nor would they be sure to know where existing safety knowledge could best be used to improve their programs.

Experience retention is an absolute necessity for effective safety programs. The "Apollo Experience Papers" requested by the Center Director at JSC are an invaluable source. Two parts of these were the Safety Experience Papers and the R & QA Experience Papers. Some of these became Technical Notes and were therefore easily available throughout NASA and the aerospace industry. This Center also prepared an Index of Safety Reports. At various Centers, Operational Readiness Inspection (ORI) documents are required for new facilities. Many of these have been published and they constitute a significant source of safety information, particularly where they discuss review procedures. For general safety information, the National Safety Council is an important source, especially for the type of information required in the establishment of a new facility.

At JSC a set of design standards has been developed from lessons learned on past programs. These standards, issued over the signature of the Center Director can be incorporated in future contracts. These go

back to the Mercury program and are sent out to all interested organizations when ready for distribution, but they may take up to six months for distribution. These are more formal than the Technical Information Bulletins which can be signed by the director of SR&QA (JSC), by the director of E & D or some comparable official, and can, therefore, bo out much more quickly.

In order to discuss to what extent safety assurance is effectively coordinated with NASA programs, it will be useful to note the organizational position of Safety offices throughout the Agency. A skeleton organization chart of safety management in NASA as it was during the time of this study, 1973, is shown in Appendix B. It is not intended to be complete, but rather to help identify specifically the offices visited in this study and others referred to in the discussion.

As noted in Section II, only selected offices were visited in the course of this study, and those shown on the chart reflect that necessarily arbitrary selection to some extent. There has been an attempt to study representative offices in OMSF, OSS, and OAST to show typical differences in organization and responsibility. The descriptions and discussions that follow are not based on an exhaustive study of each Safety office, nor do they derive entirely from official documents. The material is derived primarily from interviews with a limited number of NASA personnel in selected locations. The conclusions drawn were reached only after the members of the Syracuse research group were confident that the various points were substantiated and confirmed by remarks made or answers to direct questions given by NASA personnel, and by our own comparison of the different offices and their differing modes of operation.

B. HEADQUARTERS

The centralized responsibility for assurance functions in NASA is placed in the <u>Safety and Reliability & Quality Assurance Office</u> (SR&QA) at Headquarters. This office interacts with the five major "Offices" that cover all NASA operations: OMSF, OA, OTDA, OSS, and OAST. It also has direct and indirect relationships with all Safety and related functional offices in the major programs and at the NASA Centers. The SR&QA office is one of six staff offices in the Office of Organization and Management. This location is certainly logical and sufficiently high in the total NASA organization to provide the management overview necessary for an important centralized function. Penetration of all relevant offices throughout NASA and direct influence on their operations depend, as mentioned previously, on personal contacts and mutual respect. It seems that SR&QA has been effective in this, particularly with regard to OMSF at Headquarters, partly through the history of personal contacts and partly through the perceived importance of safety in Manned Space Flight. There is, of course, a less direct influence on the relevant offices at the OMSF Centers since OMSF has its own RQ&S office. Where there is a history of personal contact with SR&QA, notably at JSC, there seems to be unity of purpose, undoubtedly affected by other factors as well, as will be discussed later.

There are two divisions in the Safety and Reliability & Quality Assurance office at Headquarters as the name implies. The first division, Safety, has six offices: Flight Systems, System Safety, Ground Operations,

Fire, Industrial, and Awareness & Motivation. All of these provide service as requested to OMSF, OA, OTDA, OSS and OAST. System Safety, for instance, will actually work directly on a specific problem for a program or an installation as well as providing general guidance and coordination. Because requests for help clearly will be made only where the program can benefit significantly, the fact that System Safety is called upon frequently is an indication of its usefulness to the programs and of the respect granted it by many managers.

The other division of the SR&QA office is, of course, <u>Reliability and Quality Assurance</u>. Where there is a relevant office in one of the major segments of NASA, such as the RQ&S office in OMSF, the lines of communication are direct and obvious. The Office of Applications (OA) and the Office of Space Science (OSS) do not have such staff offices. For these, "Principal Specialists" are designated within SR&QA for liaison. It is interesting to note that the individual dealing with OA is designated as "Principal Specialist, Safety, R&QA," while the individual dealing with OSS is designated for R&QA only. It seems that there is ample contact between SR&QA and OA, as required, on a task-by-task basis. The significance of the title for the principal specialist in which the word "Safety" is included is that OA apparently recognizes their need for liaison in this area of assurance. By contrast, OSS apparently does not wish to consider Safety an assurance function for which liaison is required. The rejection of Safety as a parallel function along with R&QA by the Office of Space Science was borne out in our contacts with the Goddard Space Flight Center which is under OSS. See Section III. C.2.

The Office of Aeronautics and Space Technology has a Safety and
Operating Systems office attached directly to the office of the Associate
Administrator for OAST. While the relationship of this safety office to
SR&QA was not investigated in this study, there is reportedly an active
intercourse born of mutual respect and the appreciation of the importance
of safety in OAST.

Certainly the most active relationship between a major "Office" and
SR&QA exists with the Office of Manned Space Flight which has its own
staff level Reliability, Quality and Safety Office as well as RQ&S offices
in each major program at the Headquarters level. It is significant that
the present director of SR&QA for NASA came from RQ&S in Manned Space
Flight. As for the OMSF program offices at Headquarters, it is acknowl-
edged that their RQ&S offices, which must have a "solid-line" responsi-
bility to the program office, also have a "dotted-line" responsibility
to Manned Space Flight's RQ&S staff office.

It is understandable that OMSF should be more concerned with safety
than any of the other "Offices" and should see the direct relationship
between Safety and the other two assurance functions, Reliability and
Quality. It is odd, however, that while the RQ&S Office in OMSF is very
strong at Headquarters and has a close relationship with each program
office, it does not seem to have had a clear-cut influence on the relevant
offices at the three OMSF Centers, all of which are organized differently
as will be discussed.

SR&QA at Headquarters must take the lead in the dissemination of
safety information and uses several vehicles for this purpose. A NASA

Safety Alert goes out on each specific failure. Since they may deal with a contractor's proprietary information they must be cleared by the contractor legally when they deal with hardware. When they concern purely safety problems they can be put out in a week or so. They go to all Alert Coordinators throughout NASA, and it is the coordinator's responsibility to see that any affected operations and personnel are informed. This network of Alert Coordinators provides a means for rapid dissemination of any safety information. Headquarters has run a system safety course at JSC and at MSFC and Center system safety men were encouraged to attend. This was started just prior to the first Skylab launch, and it is intended that the courses continue.

One other related office should not be overlooked. That is the Office of Occupational Medicine and Environmental Health. Whereas SR&QA is at staff level in Organization and Management, this office is one of four under O & M's Institutional Management. With no solid line responsibility to SR&QA, it obviously is concerned with related medical problems as indicated by its four branches: Occupational Medicine, Environmental Health, Medical Management, and Radiological Health. These concerns were clearly not central to this study, and this office was not examined. It is mentioned to show the complexity of safety and the fact that no single office can assume responsibility for all its aspects.

In addition to this network of functional SR&QA offices, there is an entirely independent organization at Headquarters, the Aerospace Safety Advisory Panel (ASAP), which was set up at the direction of Congress as

a result of the great national concern after the AS-204 fire in 1967.
Of the nine panel members, the number of NASA personnel must not exceed
four, according to the charter. This panel reports directly to the NASA
Administrator and his Deputy and provides for them an objective overview
of management operations as they affect reliability in general, and a
critique of what led up to any particular incident. Actually, the word
"Safety" in the title is too narrow for the panel's responsibilities as
they are now interpreted, but reflects the particular concern at the
time of its formation. The panel, in fact, is concerned with technical
management (trying to assess whether NASA's managers at various levels
are looking into all the technical problems they should) and with admin-
istrative management (which deals with the timing of management's actions
and whether the right people are involved). They are concerned with both
personnel safety and mission success, but rather than being safety pro-
fessionals, they are primarily a management advisory group.

Congress is properly concerned that NASA should be a completely open
agency; the existence of this panel helps to assure Congress that NASA is
just that. ASAP is not a regulatory agency and, in fact, has no line
responsibility or authority. However, because its reports go to Congress
and to the NASA Administrator, the panel carries considerable weight.
While the panel cannot ask for funds beyond what it needs for its own
operations, it can ask for presentations, data, and so on, from others
and can say where effort should be expended.

Of the nine panel members, only two draw compensation at the present
time. The others are funded by their parent organizations from which they

obtain released time as needed. Only three staff members occupy the ASAP office at Headquarters. The panel meets monthly for two days and holds its meetings at different NASA locations in rotation or as dictated by important events.

While the panel is concerned primarily with the effect of management on safety and all other reliability factors, it has very little direct contact with the SR&QA office at Headquarters. Perhaps more frequent contact, formal or otherwise, would be valuable to both and would be particularly useful in strengthening SR&QA in NASA.

C. CENTERS

It was noted above that Safety, Reliability and Quality Assurance functions are organized and managed differently at the various NASA Centers. Even within OMSF, there is not uniformity. In the relatively small study undertaken by this group, it would have been impossible to visit all Centers or to do an intensive study of any one Center. It was, therefore, decided to visit only a few with some concentration on the two research and development OMSF Centers and with brief looks at one OSS Center and one OAST Center for contrast.

We must repeat that the comments that follow are based on rather arbitrarily selected interviews (to supplement the official publications), but that any strong opinion expressed rests on confirmation by more than one source.

1. Office of Manned Space Flight

a) Johnson Space Center

Of all the Centers visited in the study, JSC has the most effective SR&QA office. There are several reasons for this. First, this Center, formerly the Manned Spacecraft Center, has of necessity been continuously aware of the dependence of the astronauts' safety on the reliability of all systems. Being directly responsible for astronaut training as well as the command and service module, life support systems, etc., through all manned flights, and having been most directly connected with the single major fatal fire in the Apollo Program, this Center could not fail

to appreciate the importance of all assurance functions. No one in the Center director's office, in the program offices, or in the Engineering and Development directorate would have to be continuously convinced of the interdependence of safety, reliability, and quality assurance, although prior to the AS-204 fire, the Flight Safety office and the R&QA office were separate staff offices.

Second, the present director of SR&QA at JSC at one time went from this Center to Headquarters where he was temporarily in charge of SR&QA. At that time he worked closely with RQ&S in the Office of Manned Space Flight and since returning to JSC has easily maintained a good working relationship with that office and with his former colleagues in SR&QA, whose present director came from RQ&S in OMSF. Even before going to Headquarters temporarily, he had been responsible for both Flight Safety and R&QA which had not been put under one office officially then. Furthermore, the director of SR&QA at JSC is presently a consultant to the Aerospace Safety Advisory Panel.

Third, it is probably not simply chance that the Operations Safety branch is not featured in the organization of SR&QA at JSC. It is one of two branches under the Safety division, balanced by two branches under Reliability and five under Quality Assurance. The top managers in SR&QA showed that they recognize the importance of institutional or operations safety, but at the same time they recognize the stigma attached to the old-fashioned "industrial safety" engineer in the minds of technical men. To have treated institutional safety on a par with program and mission

safety might have diluted the respect this office enjoys in the programs and directorates.

Evidence of the effectiveness of SR&QA at JSC is most apparent in the close ties it has with programs and with the E & D directorate. Although the term "co-located" is rejected by some managers, it best describes the placing of an SR&QA man in another office at the Center while he still retains a position and dotted-line if not solid-line ties to SR&QA. To be specific: the director of SR&QA has three special assistants in his office, one each for Apollo, Skylab, and Space Shuttle. These three men are at the same time Special Assistants to the three respective program directors. Their appointments were approved by both the director of SR&QA and the program manager in each case, and it was evident that the program manager chose an individual in whom he had trust from past experience. Each Special Assistant has said that "wearing two hats" has not proved difficult and that there has been no conflict of loyalty or question of dual responsibility. This prime point of contact with each major program has given SR&QA unparalleled penetration of the programs in the areas of their proper concern and at the same time assured each program of complete cooperation from specialists in SR&QA when needed. The fact that these Special Assistants, while responsible primarily to their program managers, are paid as SR&QA personnel has encouraged their acceptance in the programs. The Special Assistant does not have direct authority and is primarily a liaison man with responsibility to highlight any problem he sees; he is a staff member in a program office, and since that is at the

top of the program at the Center, his perceived authority is sufficient. Both the Director of SR&QA and his Special Assistant for a particular program sit on the Level II Change Board for that program.

Since JSC is the lead center on the Space Shuttle program, the responsibility of the Special Assistant for SR&QA in this program is not limited to this Center. At MSFC there are SR&QA specialists in the Shuttle Projects Office and in each of the projects: the Space Shuttle Main Engine, the External Tank, and the Solid Rocket Booster. Each of these men while employed by Marshall with line responsibility to the office in which he is located, maintains liaison with the JSC Shuttle program office through the Special Assistant for SR&QA, who himself provides liaison to his Center's SR&QA office. The responsible individuals are thereby very effectively tied together for communication. Note that those responsible for safety in the MSFC Shuttle project offices mentioned are all out of the Q&RA Laboratory in the Science and Engineering Directorate at MSFC, not out of that Center's Safety and Manned Flight Awareness office.

In addition to the Shuttle projects at MSFC, Orbiter is a major Shuttle project office at JSC. This has an SR&QA staff man who provides liaison to the SR&QA Special Assistant in the Space Shuttle program office. Similarly, there is liaison with the SR&QA staff man in Launch Operations at KSC.

The connection between the JSC Safety, Reliability & Quality Assurance office and the Engineering and Development directorate was mentioned.

E & D does not have a Safety office. However, SR&QA personnel are assigned to each subsystem project office in E & D. These men are reportedly in on all staff meetings affecting their subsystem and they participate in Level IV Change Control Boards. Apparently they have been so well accepted in E & D that certain SR&QA men have sometimes been given the responsibility to tie all reliability functions together for the subsystem to which they have been assigned.

The System Safety branch of SR&QA at JSC, which has only six or eight people at the Center, is supported under contract by the Boeing Aerospace Company through their Houston office. For instance, Boeing had perhaps ten times that many people working on Skylab Mission Hazard Analysis. Boeing's RQA&SE office in Houston has Reliability, Quality, Safety, and Program Integration branches. From NASA's point of view, contracting for these services certainly makes sense at a time when their own personnel numbers must be kept to a minimum.

One function of the SR&QA office at JSC is to track all assurance operations at contractors' and sub-contractors' plants through assignment of their own men to these plants. This was true in the Apollo Program also. The resident SR&QA men submit weekly reports to the Center's SR&QA office where they are assembled and forwarded to the relevant program manager.

To combat a series of industrial type accidents at JSC, hazard identification courses were set up and presented on an informal basis to bring technicians together with accident investigating board chairmen.

They discussed real problems that had occurred, filmed some of the sessions, and have now achieved the point at which contractor people can run their own programs. Another educational effort of SR&QA at JSC was the production of a series of Safety Kits dealing with a wide range of commonly encountered problems. The use of posters and pamphlets was employed to spread easily-understood information to a wide audience at the Center.

An important but seemingly obvious device is utilized at JSC to facilitate communication among groups with overlapping assurance responsibilities: offices such as Systems Integration, Flight Systems Integration, Ground Systems Integration, Flight Safety, and SR&QA are located close together in the same building. Because NASA's facilities are spread so widely geographically, and even at one Center offices can be very far apart, this logical type of grouping is not always found elsewhere. There is bound to be overlap in the responsibilities of closely-related offices. For instance, the manager for Flight Safety must pursue the cause of a test failure while SR&QA personnel must document that failure and its resolution. Rather than being a disadvantage and a duplication of effort, this can be (and at JSC apparently is) an opportunity for one office to support another with exchange of data and complementation of personal capabilities. The juxtaposition of related offices certainly encourages such mutual support and may be a contributing factor in encouraging the apparent close cooperation among the individuals in the offices mentioned.

b) <u>Marshall Space Flight Center</u>

The office responsible for safety at the Marshall Space Flight Center is called <u>Safety and Manned Flight Awareness</u>. It is one of several staff level offices, in essentially the same position in Center organization as is Safety, Reliability & Quality Assurance at JSC. One major difference between the two is indicated by the title of the office which has no direct responsibility for reliability and quality assurance. There is no staff level office for R & QA. There is in-house competence in that area in the Quality and Reliability Assurance Laboratory in the Science and Engineering Directorate. In addition, the Systems/Products Office at staff level in Science and Engineering has a management responsibility to be sure that the proper person or group in S & E is studying any particular safety or reliability and quality problem. Total responsibility for these assurance functions is therefore not concentrated at one place, high in the Center organization; liaison among the offices concerned is maintained through considerable effort.

The Safety and Manned Flight Awareness Office has a deputy director for each of its two responsibilities: the safety side has branch chiefs for System Safety, Industrial Safety, and Research & Evaluation; the Awareness side has only the one section. This latter responsibility, Awareness, is essentially a motivation generating source, concerned, as the name implies, with keeping both NASA and contractor personnel at all levels aware of the critical nature of each major and minor task in view of the potential danger to the astronauts in any system failure. One

effort of the Manned Flight Awareness Office was an Error Cause Identification and Removal program with the contractors. Goals were set, and then publicized with posters, an exhibit van, visits from astronauts, etc.

MSFC is the only Center with a Manned Flight Awareness office and its responsibilities are NASA-wide, at least for manned programs. At the same time, there is an Awareness and Motivation office under the director of the Safety Division of SR&QA at Headquarters as previously mentioned. The newsletter, Awareness, comes from that Headquarters office, and their special advisor for the new Aerospace Awareness Program, Systems and Applications Techniques is from the Kennedy Space Center. NASA is in the process of establishing Aerospace Awareness offices at Centers other than those of OMSF.

MSFC's organizational management of safety-related assurances is strongly influenced by the history of the Center. The laboratories in the Science and Engineering directorate (formerly Research and Development Operations) have always been very strong, representing one of NASA's greatest in-house capabilities, and have always influenced Center policy greatly. Before the AS-204 fire in 1967, Safety was under Management Services and was essentially industrial safety, associated with the personnel office and run with the aid of a support contractor. In 1968 Safety became a Center staff office and Manned Flight Awareness was in the Industrial Operations (later Program Management) directorate. Safety and MFA were combined and then moved to the present staff position when the PM directorate was abolished. During all this, there was no direct connection (solid line) with Quality and Reliability Assurance which remained in the Laboratories.

MSFC has reportedly used Failure Mode and Effect Analysis (FMEA) in depth on various projects for some time now. Because of the Center's past concern primarily with boosters, they seem to have shied away from the "human element" in safety analysis. Their Design Guide does not deal with this element.

Certain safety analysis work at MSFC is presently contracted out. The Martin Marietta Corporation through its Huntsville office has conducted studies for the Skylab systems, just as Boeing has done for JSC at Houston. Again, the desire to keep NASA offices at a minimum stable manpower level requires that large studies of short duration be contracted out.

When a Q & RA man works on a problem in a program or project, he continues to be paid by institutional funds through his home laboratory in accordance with a Task Agreement, which is a more formal procedure than had been used in the past. Each laboratory has a Safety Project Engineer who is laboratory based and not responsible to the Center's Safety office. The Systems/Products office in S & E does have a Safety Engineering office, and S & MFA's contact with all safety efforts in the laboratories is through the deputy director for Systems/Products where, as mentioned, the management responsibility for these safety efforts resides.

There seems to be a close working relationship between the director of S & MFA and the deputy director of Systems/Products. Nevertheless, the relationship is not structured by formal sign-off or other line

responsibility for the S & MFA office. There is similarly no sign-off authority granted to Safety or Q & RA men in projects or programs. Neither are there Safety men co-located in program offices. Although each program has some Safety office, that office has no formal ties to the Center's Safety office. Formal ties to program offices is the greatest limitation on the efforts of the S & MFA office. It is true that the director of S & MFA has the right to sit in on any Level II reviews and has no difficulty making himself heard on any safety-related issue. As with any other NASA officer, his influence then depends on his personal powers of persuasion and he is certainly helped by being organizationally very high at the Center. Nevertheless, he lacks the day-to-day contact with program problems and very easily can be taken by surprise and be less prepared than he would like to be by an unexpected agenda item. In other words, the S & MFA office does not sufficiently penetrate the major activities of the Center.

It seems that at MSFC a large part of the continuity of knowledge from one program to another has depended on personal discussions both formal and informal among higher level management executives. This applies to SR&QA experience as well as other technical and managerial know-how. Quite obviously this is not as complete and reliable a transfer of knowledge as could be assured by an adequate management structure, especially since many key managers from the Apollo and other programs continue to retire.

2. Office of Space Science: Goddard Space Flight Center

The Goddard Space Flight Center is under the Office of Space Science. The description of safety activities at Goddard and the comments made here are based on a brief visit there by two members of this study group early in 1973. At that time, the Chief of the Health and Safety Engineering Office and the Chief of the Safety section of that office, as well as the Associate Deputy Center Director, Engineering, were interviewed. In addition, the Goddard Management Instructions were reviewed with particular attention to Appendix C which deals with safety responsibilities. While the remarks to follow are necessarily cursory, and while Goddard's safety activities are not precisely the same as those in other OSS Centers, it is considered useful to include this section of the report for some comparison with the more detailed discussion of OMSF Centers.

The Office of Health and Safety Engineering (H & SE) nominally is responsible for both project system safety and institutional plant safety. It is divided into a Health and Environmental Section and a Safety Section. The primary function of the Safety Section is seen to be the encouragement of the development of a System Safety Plan by project management before the beginning of each new project. The requirements for the System Safety Plan and for an implementation plan are formalized in Appendix C of the Goddard Management Instructions (GMI) and that Appendix was, to a large extent, the result of efforts by the Safety Section of the H & SE office.

The Appendix C provisions describe the scope and purpose of the required Safety Plan and include definitions of safety terminology. An

outline of the Safety Plan as well as examples of standard safety documents are presented. The appointment of a project Safety Officer is required, and his responsibilities as the focal point for overall systems safety are outlined. The Safety Plan must indicate how it is to be coordinated with the Health and Safety Engineering Office concerning that office's industrial safety responsibilities and its integrated total Safety Program. Monitoring of the progress of the Safety Plan is effected by requirements such as safety audits, design reviews, mishap reporting and waiver procedures.

While compliance with the general provisions of the GMI manual are supposedly assured by top Center management, it is apparent that these procedures are not considered by some engineering and project managers to be absolutely vital. It is not clear what enforcement powers reside with the Health and Safety Engineering Office. The office is responsible for Health and Environmental Safety for which the medical functions are carried out by physicians under contract. The general plant safety or industrial safety operations are clearly the responsibility of H & SE. It is only in these areas that the office seems to have real responsibility and autonomy. It seems the project and center managers are inclined to view health matters and industrial safety as the proper and perhaps only concern of the H & SE office.

At least some managers at the Goddard Space Flight Center view safety assurance as an integral part of the project manager's job and feel that good engineering results in good safety assurance to the extent allowed by currently restricted budgets. The Reliability and Quality

Assurance Office, which is completely separate from Health and Safety
Engineering, is considered to be only advisory to the project offices.
Goddard has always placed great reliance on testing and well-developed
test procedures. Of course, their record of locating and correcting
troubles through test is remarkably good. But testing to the extent
that it was done in the past is expensive and testing must come at a
relatively late stage in system development. With current budget
limitations, it is important to prevent major redesign expenditures on
potentially troublesome components and systems.

Management recognizes, of course, that system quality control is
essential, and there is a system engineer on each project, but any
imposition of system safety analysis by an outside safety-oriented
group is apparently resisted. The establishment of a formal system
safety review procedure is resisted by several arguments: R & QA pro-
vides an alert system during the development of a project, and design
reviews are intended to assure the adequacy of any design or change,
to check on contractor progress, and to review test specifications.
Also, Goddard personnel feel that there is additional protection in
the fact that KSC has its own safety group that must be convinced of
the safety of any change made before launch. The development of the
type of specialized systems coming out of Goddard is a continuously
iterative process, reviewed by their own designers at every step.

Of course, it must be noted that Goddard is not directly concerned
with the development of man-rated systems. Their own experience shows
that there is seldom total failure of a system and that missions can
often be accomplished even with partial failure. With the current

budget restrictions, there is a feeling that the goal must be adequate performance at low cost and that NASA must be prepared to accept more risk in unmanned missions. One way of achieving lowered costs is to save the expense of system safety analysis; this view is apparently becoming more prevalent.

Goddard is not quite so averse to system safety studies as they appear to be on the surface. They have in fact obtained assistance from the Headquarters SR&QA office for detailed studies of specific problems. But this type of ad hoc arrangement cannot effectively replace the potential benefits of an ongoing Center activity in this area. As previously stated in this report, safety assurance, well-coordinated with the other assurance functions, should be involved in projects and programs from their inception and the office coordinating these activities as well as being available to project directors should be highly placed in the management structure to have an effective voice in the various phases of development and review.

3. Office of Aeronautics & Space Technology: Lewis Research Center

The safety-related activities at Lewis can be broadly classified into three groups which are organizationally independent. The first of these is the Safety and Project Planning Office under the Technical Services Directorate. The second is a group which can be broadly described as "Safety Committees." The third, the ASRDI organization, headquartered at the Lewis Research Center, is definitely a safety-related group, but since its mission is NASA-wide, rather than Lewis-oriented, it will be

examined separately in another section of this report (Chapter IV).
Finally, the Office of Reliability and Quality Assurance, although it is
obviously responsible for some safety-related problems, was not included
in our study of safety problems at Lewis.

While the chief objective of our two visits to the Lewis Research
Laboratories was a study of ASRDI, a secondary objective was to examine
the functions of the Safety and Project Planning Office along with the
"Safety Committee" structure. To carry out this secondary objective an
interview was arranged with the chief of the Safety and Project Planning
Office under the Technical Services Directorate. This meeting was
designed to help gain insight into the safety-related organization at
Lewis which was independent of the ASRDI operation. Other information
about these activities was also obtained during conversations with ASRDI
personnel and through the direct working experience of one of the authors
during the tenure of an ASEE/NASA Summer Faculty Fellowship in 1972.

Safety and Project Planning Office

The Director of the Safety and Project Planning Office is responsible
for implementing much of the Lewis Research Center's Operations Safety
Program which is designed to meet the needs and requirements at this par-
ticular Center. The basic operation of Lewis is research and development,
and the safety operation reflects such an orientation. The Safety and
Project Planning Office is responsible for the prevention of loss of life
and property in both institutional and project-related operations. Its
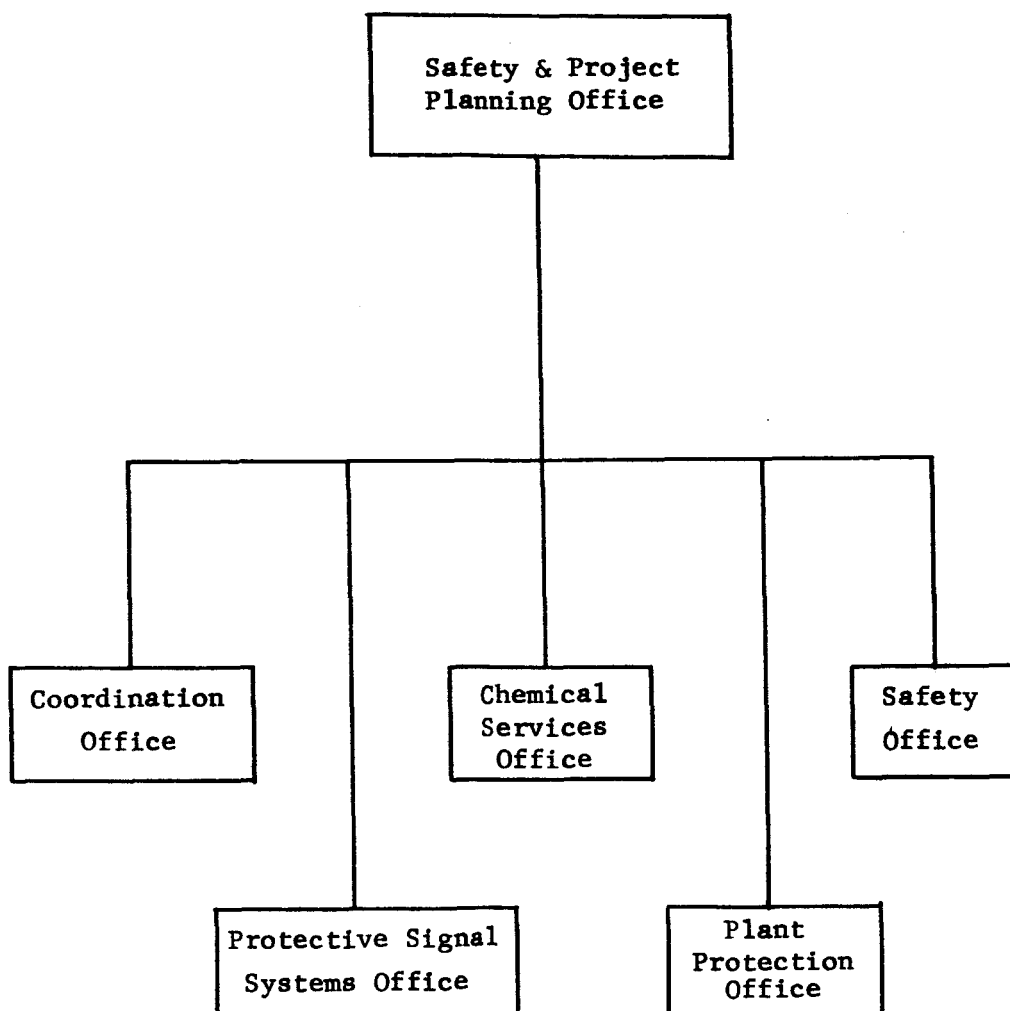five key offices, shown in Figure 1, are described below.

Figure 1. Organization of the Safety Project Planning Office
Lewis Research Center

A. <u>Coordination Office</u>. The responsibility of this unit is to assist in coordinating various safety-related activities at Lewis. This Office also supports the research engineers in their attempts to get their projects on-line through the phases of procurement, fabrication, etc. A purchase request, for example, may be reviewed by the Coordination Office to make sure that safety requirements are met. The Coordination Office reviews approximately 90% of all the Center's purchase orders to evaluate the implications for safety. Work orders to install a piece of equipment may also be reviewed for their potential impact on safety. If a purchase request for a piece of equipment or hardware does not meet safety standards it normally will be returned to the originator or some other safety committee for further evaluation.

B. <u>Protective Signal Systems Office</u>. This office is responsible for automatic monitoring devices, gauges, etc., whose purpose is to warn of potential dangers arising from hazardous operations.

C. <u>Chemical Services Office</u>. The responsibility of this unit is centered around analytical work and research on gas chemistry. The office was an outgrowth of the need to fulfill a specific safety requirement at the Lewis Research Center.

D. <u>Plant Protection Office</u>. The responsibilities of this office include protecting life and property in and around the physical plant, buildings, and grounds at Lewis. The Center's fire fighting force comes under their cognizance.

E. <u>Safety Office</u>. This safety activity is closely related to the operations safety programs similar to those found in industrial safety practice.

A major function of the Safety and Project Planning Office is in the area of what has been called "operations safety." The focus of operational safety is on the protection of life and property; this of course, includes accident prevention. When a hazardous operation must be conducted which contains a potentially dangerous operation, a Safety Permit to proceed with the operation must be obtained. Upon application for a Safety Permit, the planned operation is normally reviewed for possible omissions of important safety procedures or the presence of hazardous materials, etc. Personnel from the Safety and Project Planning Office may be involved either directly or indirectly. The Safety Permit serves as a control device for those charged with the safety of the operation. A Safety Permit, for example, requires information on what is required and who will be responsible for the task (e.g., handling explosive gases), and what procedures will be used in accomplishing the task. The safety personnel have the right to stop a project if negligence is observed. The grantor of a Safety Permit may be one of several offices or committees, such as an Area Safety Committee, the Systems Safety Committee, or some part of the Safety and Project Planning Office, depending on the nature of the task. A copy of every Safety Permit issued is kept in the S & PP office.

Once the permit is issued to proceed with a potentially hazardous operation, the appropriate group will continue to review the work being performed and discuss safety-related items with supervisors, technicians and workmen. Such surveillance helps insure that safety standards are kept current and are being followed correctly. The nature of a task determines which group should be responsible for issuing a Safety Permit to carry out the task.

Safety Committees

An extensive system of committees and panels, all dealing with safety-related topics, has evolved at the Lewis Research Center. These groups include the Executive Safety Board, the various Area Safety Committees, the technical specialist Advisory Panels, and other miscellaneous groups such as the Process Systems Safety Committee, Accident Investigation Committee, Special Electrical Applications Safety Committee, and the Radiation Safety Committee. The organizational relationships of these groups are not well defined, but the Executive Safety Board oversees general safety operations and the work of the various groups is coordinated to the extent that committee membership overlaps and personal acquaintances are utilized. The basic functional responsibilities of some of these groups will be briefly described.

A. <u>Executive Safety Board</u>. This group acts as an advisory staff to the Center Director on all safety-related matters. It provides an overview of all safety operations to insure that safety programs planned at Lewis are implemented. All Area Safety Committee and Advisory Panel Chairmen meet with this Board at least once per year to discuss programs. The Board has been described as similar in function to the Aerospace Safety Advisory Panel at Headquarters, although ASAP is less operationally oriented than the Lewis group. The membership of this panel is drawn from high-level management personnel of the various directorates at Lewis, usually the directors themselves. The Director of Center Development, is

Chairman of the Executive Safety Board. The committee has seven members including the Lewis Safety Officer who is automatically Executive Secretary of the Executive Safety Board. The Board can request written inputs from any of the Area Safety Committees or Advisory Panels when it identifies a safety problem which it feels has not been adequately treated.

B. Area Safety Committees. These groups consist of professional specialists from various fields working together as equals. The committees are responsible for experimental programs within their particular physical area of the center. These areas are precisely defined on a map of the Lewis Research Center which is included, among other places, in the LRC telephone directory. Their responsibility involves the evaluation and approval, from the point of view of safety only, of all proposals for new experimental programs or major changes to existing programs. Outside specialists are called in if needed. Advisory Panels of specialists may also be questioned by the Area Safety Committees. Approval of the Area Safety Committee in the form of a written permit is required before the program can begin operation. There are seven Area Safety Committees at Lewis and there were four at the Plum Brook Station. The Lewis Safety Officer is an ex-officio member of all Area Safety Committees.

C. Advisory Panels. There are five Advisory Panels which bring staff together with special expertise. The topical areas of organization of the panels are: Construction, Experimental Fluids and Gases, Fire Protection Systems, and Utilization and Standards for High Pressure Gas and Cryogenic Containers. These panels can interact with the Area

Safety Committees. A dissenting opinion can be issued as a memorandum
to the Executive Safety Board. Each permit issued by the Area Safety Com-
mittee has a space on it to identify all Advisory Panels utilized in re-
viewing the permit application. In this way the role of other groups is
publicized. The most frequent use of the Advisory Panels is for review
of an Area Safety Committee permit. Anyone else can consult with the
Panels for pre-permit design advice and this is usually done informally
through one of the Panel members. The Advisory Panels have an important
additional flexibility in that they can identify safety problems on their
own initiative and investigate formally. This aspect of their work is
limited only by their initiative and their lack of independent budgetary
authority. Although the Advisory Panels' areas of concern are broader
than safety alone, their objectives are primarily safety since the assur-
ance of designed operation is a safety-related function.

D. <u>Process System Safety Committee</u>. This is a recently formed com-
mittee (July 1973) created by the Center Director and chaired by the
Director of ASRDI. This group reviews all large, complex systems with
multiple users to identify potential hazards in the system, especially
those caused by changes. The committee came about in part as a response
to the inability of the Area Safety Committees to deal effectively with
systems which crossed area lines. There was a common tendency to regard
systems and experimental facilities as separate. Any system which, for
example, delivers fuel, air, etc., to a test facility will automatically
come under the review of the Process System Safety Committee when the

Director of Engineering Services notifies them of changes. This review can include design features, operations and communications. This committee must issue an operations permit for the system, usually in conjunction with the appropriate Area Safety Committee, although usually not related to any request for an Area Safety Committee permit. The membership of the Committee is generally derived from a higher organizational level than the Area Safety Committee membership.

E. <u>Accident Investigation Committee</u>. This Committee is available to conduct a formal investigation of personal injury and property loss accidents when requested by the Executive Secretary on behalf of the Executive Safety Board. The guidelines for initiating an investigation are generally those suggested by the Headquarters classification of accident categories. The Executive Secretary can go beyond the administration-wide requirements and have lesser accidents invesitgated. Near-misses apparently fit into this latter category, but these cases must rely on individual knowledge and interest in the near-miss in order for action to be taken.

F. <u>Special Electrical Applications Safety Committee</u>. This Committee recently replaced the former Advisory Panel of the same name. It is meant to be a parallel organization to the Process Systems Safety Committee to deal with large electrical supply systems. As a committee, it is able to control new or modified electrical projects through the permit system, a function it did not have as an advisory panel.

Trends in Safety Management at LRC

It seems clear that an understanding of the importance of good safety practices has become an integral part of the Lewis operations for three principal reasons. First, the Apollo AS-204 fire gave safety both visibility and priority at all NASA Centers; this resulted in better organization of all forms of safety operations from top management downward. Second, as activities and projects have become more complex, more stringent and sophisticated safety management was required. Third, the recent enactment of the Occupational Safety and Health Act (OSHA) has made all Centers more aware of the importance of effective safety practices in day-to-day operations. While OSHA regulations do not directly apply to the type of work done at the Lewis Research Center, directives have been issued requiring Lewis operations to be consistent with OSHA standards, and the Lewis Safety Office has been given the staff to implement these requirements.

A trend is also developing at Lewis to embrace the concept of integrated Systems Safety wherever possible. As projects, interfaces, and technology have become more complex, safety management concepts also have had to change. At Lewis, systems safety now begins in the design phases of a project in the belief that good design is an essential step in the prevention of accidents. Systems safety requires the continual review of the entire system and its components, such as the mechanical subsystems, the electrical subsystems, and the "human" subsystems.

There are several groups and committees responsible for implementing systems safety concepts at Lewis. Usually the Area Safety Committee and

the Systems Safety Committee are both involved. Generally, approval of a new design, test, or major operation requires both groups to concur on the soundness of a given proposal. The Chief of the Safety and Project Planning Office serves as an ex-officio member on both the Area Safety Committees and the Process Systems Safety Committee, thus tying the two together.

At Lewis, systems safety concepts are primarily oriented towards in-house research and development projects and operations, including the specialized equipment and facilities of this center. In contrast, the emphasis at JSC and MSFC is on applying systems safety concepts to man-rated projects for space flight.

Summary and Critique

The committee and panel structure as it has evolved at Lewis is unique in the NASA organization -- if not in kind, at least in degree. The basic flexibility of the arrangement is probably appropriate for a research-oriented operation of the Lewis type under the Office of Aeronautics and Space Technology since these centers are concerned with diverse, large and small experimental programs and major test facilities which do not correspond with the programmatic safety problems characteristic of the Office of Manned Space Flight.

The coordination of activities between the various committees and panels, to the extent to which it is needed to achieve overall administration or Center safety objectives, is provided by the Executive Safety

Board. As described earlier, the Executive Safety Board's Executive

Secretary is also the Lewis Safety Officer. As Safety Officer and Chief

of the Safety and Project Planning Office, he is also an ex-officio member

of each Area Safety Committee. This multiple role for one individual pro-

vides coordination, but also has been found to create uncertainty for

laboratory-level staff concerning whether they are dealing with an Area

Safety Committee or the Safety and Project Planning Office when a permit

is being sought for a new or changed facility. Such ambiguity may not

now be serious, but is potentially a detriment to safety operations. The

difficulty of attending each Area Safety Committee meeting with limited

staff is also a problem for the Safety Officer. Decisions must often be

made to predetermine the importance of the meeting to evaluate whether it

is necessary for the Safety Officer or his representative to attend. This

decision should not have to be made.

Of concern to the Syracuse Study Team is the lack of formally estab-

lished relationships among the various Lewis Safety Committees and Panels.

It appears that the integration and coordination of the various Committees'

efforts is primarily accomplished on an ad hoc basis through the interper-

sonal relationships of the various members. We question whether this is

good management policy. An important strength to be derived from estab-

lishing these formal relationships and policies is that it could help

insure the continuity and completeness of a committee's efforts.

We also have been concerned about the real role of the Project Plan-

ning and Safety Office. The question we raise is whether this Office is

truly involved in the planning of safety for projects, or does the Office perform the role of expeditor in procurement, etc. Our interviews revealed that there were some conflicting opinions on the extent of this Office's safety role in project planning.

A final point which should be raised is the extent of the decentralized activities which are organized under the Lewis Safety and Project Planning Office. Decentralization of any management activity helps in establishing a point of responsibility for that activity. As a consequence, accountability can be more readily identified and established. On the other hand, too much decentralization can waste both human and materiel resources. We question whether all the separate activities which have been grouped under the Safety and Project Planning Offices do require the separate, small organizational units. A close examination of the functions each "office" performs might reveal that a consolidation of these activities is needed and would promote efficiency.

IV.   ASRDI:[*]   THE MANAGEMENT OF SAFETY INFORMATION

A.   SUMMARY OF FINDINGS AND RECOMMENDATIONS

Effective safety technology and information transfer requires a
systematic process consisting of a source of information and technology,
a middleman, and users with feedback to the source. The Syracuse Univer-
sity research group has analyzed ASRDI in terms of seven elemental func-
tions which would have to be performed for the successful operation of
the transfer loop. In this report, our observations and recommendations
have been highlighted in terms of each of these elements. The following
points summarize these findings and recommendations.

1. It is our belief that the prime barriers to more effective
functioning of ASRDI are: a) lack of funds for operation and travel,
b) lack of a unified funding source, c) conflicts in priorities, d) lack
of visibility, and e) insufficient staffing.

These are clearly interrelated and not mutually exclusive problems.
Until adequate and unified funding is provided and staffing restrictions
are removed, it will be difficult for ASRDI to improve its visibility
and to assume an aggressive posture. Some NASA managers believe that
ASRDI could get the needed resources if they could prove their worth as
"information brokers." However, they would certainly have to be "self
starters" within the competitive management system of NASA. ASRDI feels

_____

*ASRDI is the acronym for the Aerospace Safety Research and Data
Institute, located at the Lewis Research Center, Cleveland, Ohio.

it does not have the resources to do its job; at the same time others seem

to be saying that ASRDI will not get the resources until they prove them-

selves. This cyclical argument has to be broken.

2. There appears to be a lack of agreement within NASA as to the

objectives of ASRDI. Divergent points of interpretation of ASRDI's charter,

particularly research versus information transfer, should be resolved. The

present operation is too small to do both effectively. For maximum effec-

tiveness under present conditions, we believe ASRDI should concentrate on

the information transfer function.

3. We believe that the present system of information organization

is neither well founded on user needs and priorities nor on program/project

management expectations and priorities. Due to resource limitations it is

difficult to satisfy both general and specific information needs of a diverse

group of users. The present system can be improved by conducting a market

survey of NASA's realistically foreseeable information needs at various

organizational levels so that the information system that is built can con-

form to these needs.

4. ASRDI should continue to pursue specific and active transfers

wherever possible. It appears that information such as that pertaining to

oxygen/cryogenic technology was more effective than the transfer of more

general types of information. However, some attention must still be given

to generally useful safety information and ASRDI must respond to calls

from within NASA and NASA-related industries seeking help on general safety

measures.

5. As technological information originators, ASRDI is more research-oriented than information/dissemination-oriented. Since neither the originator nor the user usually performs the middleman or broker function well, we have suggested the establishment of Safety Application Teams along the lines of NASA's Biomedical or Technology Application Teams. The SAT teams could interface both with NASA flight and non-flight systems and other programs, identify needs, and match available technologies to these needs. In addition, they could transfer information and technology in a manner which more nearly fits a particular user's need. We also recommend a more formalized analytical approach to the collection and documentation of safety related accidents/incidents to reveal patterns of voids and needs.

6. We recommend a change in the staff mix through the addition of multidisciplinary personnel with engineering/communications backgrounds and the type of personnel who would make ASRDI more of a service agency rather than a research agency.

7. We recommend that ASRDI should broaden its policy of interagency-personal interaction. While there are other methods to disseminate safety information, it is our firm belief that interacting with as broad a spectrum of people as possible is the best way.

8. A formalized contact point at various program and project centers will make communicating and the transfer of information between these centers and ASRDI more systematic.

9. Safety dissemination by ASRDI can be improved by more extensive use of the facilities of existing Regional Dissemination Centers.

10. Organization structures and practices do affect the transfer process. We recommend the issuance of a NASA Management Instruction Sheet formalizing ASRDI's responsibilities and defining relations with other Program/Project Safety centers and Headquarters. Today it exists as an organization without clearly delineated responsibilities and accountability.

11. Shifting ASRDI out of Lewis and into Headquarters would give ASRDI better visibility and accessibility. It would also improve communications with the Safety and Reliability and Quality Assurance office at Headquarters, making operations more effective. Even if a physical shift is not possible, at least organizationally ASRDI should report to the Headquarters SR&QA office rather than to Lewis. We will in this section of the report look at the pros and cons of this issue. We must point out that some people felt that ASRDI would be better left at Lewis and that this was in line with NASA's overall policy of limiting the direct control by NASA over such organizations as ASRDI.

12. On the question of planning for the present and future, we recommend that:

      a. ASRDI draw up a comprehensive plan detailing their
            present capabilities to resolve the question of
            what their objectives will be: pure research or
            pure information transfer or some judicious mix of
            both and their priorities.

      b. ASRDI draw up a long-range plan of the kinds of in-
            formation and services users will need -- what areas
            of data need to be collected, analyzed, and stored
            for dissemination.

c. ASRDI devise a formalized feedback system to monitor
    and control discrepancies.

d. ASRDI develop a set of performance measures for self-
    evaluation to gauge the effectiveness of the job they
    are doing in terms of information transfer.

B. INTRODUCTION

The study of the Aerospace Safety Research and Data Institute (ASRDI) was part of the broader study undertaken by the Syracuse/NASA research group on Safety Management in NASA. This section of the report focuses on the management and transfer of Safety knowledge from ASRDI to other NASA Centers, from one program to another, from ASRDI to other Governmental agencies and contractors, and from ASRDI to the private sector. A broad perspective is taken in analyzing what is being done and what can be done to improve the management and transfer of safety knowledge from ASRDI to potential users of safety information. Figure 2 on page 59 shows schematically how an information support system, such as ASRDI, interacts with others.

This section first reviews the purpose for which ASRDI was established and its objectives and then looks at existing organizational arrangements-- staffing and funding--for the research and transfer of safety information. One of the problems in applying safety concepts at other centers, in other programs, and in industry at the appropriate time is the general failure to communicate effectively and transfer the knowledge accumulated.

The section examines what techniques are available to collect, identify, match and disseminate information and what ASRDI has done in terms of projects undertaken. Several ASRDI studies are highlighted to illustrate key points. Problems and barriers that exist in the information collection, analysis, and dissemination process are also explored. In examining ASRDI's various organizational relationships, the study focuses on how ASRDI inter-
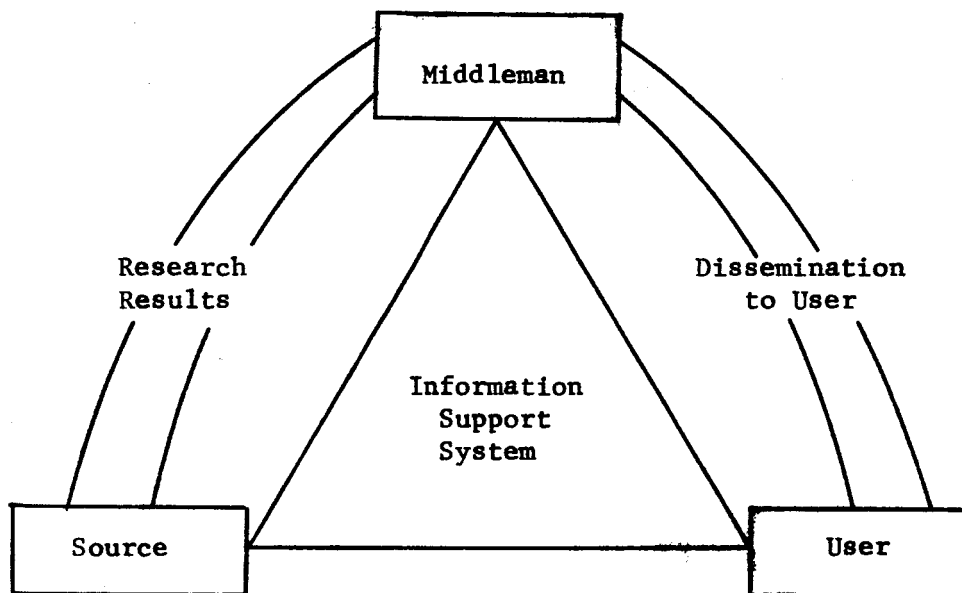
Figure 2.   Framework of a Safety Information
Transfer System[*]

* Adapted from: Heinz Dinter, "A Man-Machine System for
Transfer of Research Knowledge to Industry," Business and
Economic Dimensions, Vol. 3, No. 5 (May, 1967), p. 6.

faces with other NASA safety groups such as JSC, MSFC, KSC, ASAP, various NASA safety review boards, and external organizations. Finally, specific recommendations are made for facilitating the collection, identification, matching, and dissemination of safety information which may be useful to ASRDI and other safety organizations.

As explained at the beginning of this report, the information has been obtained through interviews conducted by two- to three-man inter-disciplinary teams from Syracuse University with key personnel within ASRDI at the Lewis Research Center and at other NASA centers. Both structured and unstructured interview formats were used. Even though some interviews were taped, the process did not appear to limit or inhibit the discussion or remarks of the interviewees due to the confidentiality that has always been accorded such interviews in the past. Various NASA documents were studied, and many points were clarified through telephone conversations.

Experience gained by this group in previous studies (Syracuse/NASA Project Management Study) was utilized in making contacts. This report is thus an outcome of several research approaches as well as debates and ex-changes of opinion among members of the Syracuse team. We were fortunate in having the cooperation of the personnel at the Lewis Research Center in Cleveland, at Headquarters and at various NASA centers.

C. ESTABLISHMENT OF ASRDI

ASRDI was formed in 1968-69 in response to the Apollo AS-204 fire. NASA's chief administrators and Congress felt that NASA needed one organization where safety information could be collected, validated, researched, updated, and interpreted for use by NASA safety offices, the aerospace industry, and other potential users. Although the initial idea was to establish ASRDI in Washington, D. C., certain managerial, personnel, and allied problems eventually made Washington inconvenient. In addition, since research was to play a vital role in the whole process, it was felt that ASRDI should be established where appropriate research facilities would be available. Therefore, the Lewis Research Center was eventually chosen as the ASRDI base.

According to NASA's top administrators when the Institute was set up, ASRDI's functions were:

a. To establish and operate a safety data bank, to evaluate critically existing information going into the data system for storage, and to add to it (update) on a regular basis.

b. To support and furnish with technical information other NASA safety centers, contractors, Government agencies, the aerospace industry and other agencies, and also to consult on safety problems.

c. To research and analyze where safety problems and technology gaps exist and to initiate research programs both inside ASRDI and via contracts with outside vendors in these problem areas.

d. To prepare advisories (problem-oriented briefs), state-of-the-art summaries (such as the oxygen series), and educational material (movies, papers, publications).

e. To apply systems safety analysis and data to specific projects.

It seems worthwhile to consider more extensively the "objectives" for which ASRDI was established because there seems to be some divergence of opinion on the current interpretation of these objectives. Some personnel, for example, in the NASA Headquarters Safety Office, feel that ASRDI should devote more time to collecting and disseminating safety knowledge and consulting with users of safety information. Other personnel at various safety centers feel that ASRDI is getting involved in areas that are not relevant or helpful to them. While Headquarters is aware of the importance of research, it seems to be giving it a minor role since ASRDI does not have adequate staff or the types of people to carry on safety research on a large scale.

ASRDI personnel feel, on the other hand, that research is basic to their fundamental purpose. Many of the personnel who initially joined ASRDI did so because it was to be basically a research organization. If it had been designed solely as a data collection operation it could as easily have been situated at Headquarters. According to the personnel at ASRDI, research and data are both interwoven because research suggests what data to collect which, in turn, indicates important research gaps in safety information. Some questions about safety have been asked to which answers are not available for lack of research, while many more questions have not yet been asked. This is where ASRDI's research role is important -- ASRDI helps provide questions as well as answers. Thus, ASRDI personnel indicate that spending full time collecting and disseminating safety

information conflicts with the time they can devote to research. Observation of their staffing confirms that ASRDI personnel feel they should be more of a research than a dissemination agency. The present operation is too small for both research and effective dissemination of information.

We feel that both must be done but that the safety research should be, for the most part, contracted out by ASRDI, preferably within the NASA organization. In addition, ASRDI itself should do a modest amount of safety research where its existing personnel and facilities warrant. Reports from the field centers and Headquarters seem to strongly favor more emphasis on collection and dissemination rather than research.

To handle its responsibilities, ASRDI had a staff of 19 at the beginning of 1973. It was down to 13 as of July 1, 1973, due to recent personnel cutbacks. There are sixteen areas where ASRDI personnel possess special talents and experience relevant to safety technology, and their location at Lewis gives them access to other specialists, when needed, on a consulting basis. On the other hand, some of the ASRDI specialists have been temporarily utilized for outside activities, depleting the already thin ASRDI staff. Among the staff of 13, there are only three who are specialists in information dissemination, while the rest are specialists and researchers in various technical fields. Three information specialists in an agency where one of the important jobs is transfer of information are certainly inadequate.

Funds for ASRDI come from OAST through three of its divisions, namely:

    a. Aeronautical Operating System Division

    b. Applications Technology Office

    c. Space Propulsion & Power Division

Through the courtesy and interests of some of the aerospace firms, research work in other safety-related areas has also been conducted. ASRDI funding is for the most part project-oriented. The mode of funding has contributed to the limited effectiveness of the Institute. A unified, single source funding could help ASRDI provide better direction, priorities, and coordination of their efforts. Figure 3 on page 65 illustrates the ASRDI funding arrangements as of early 1973.
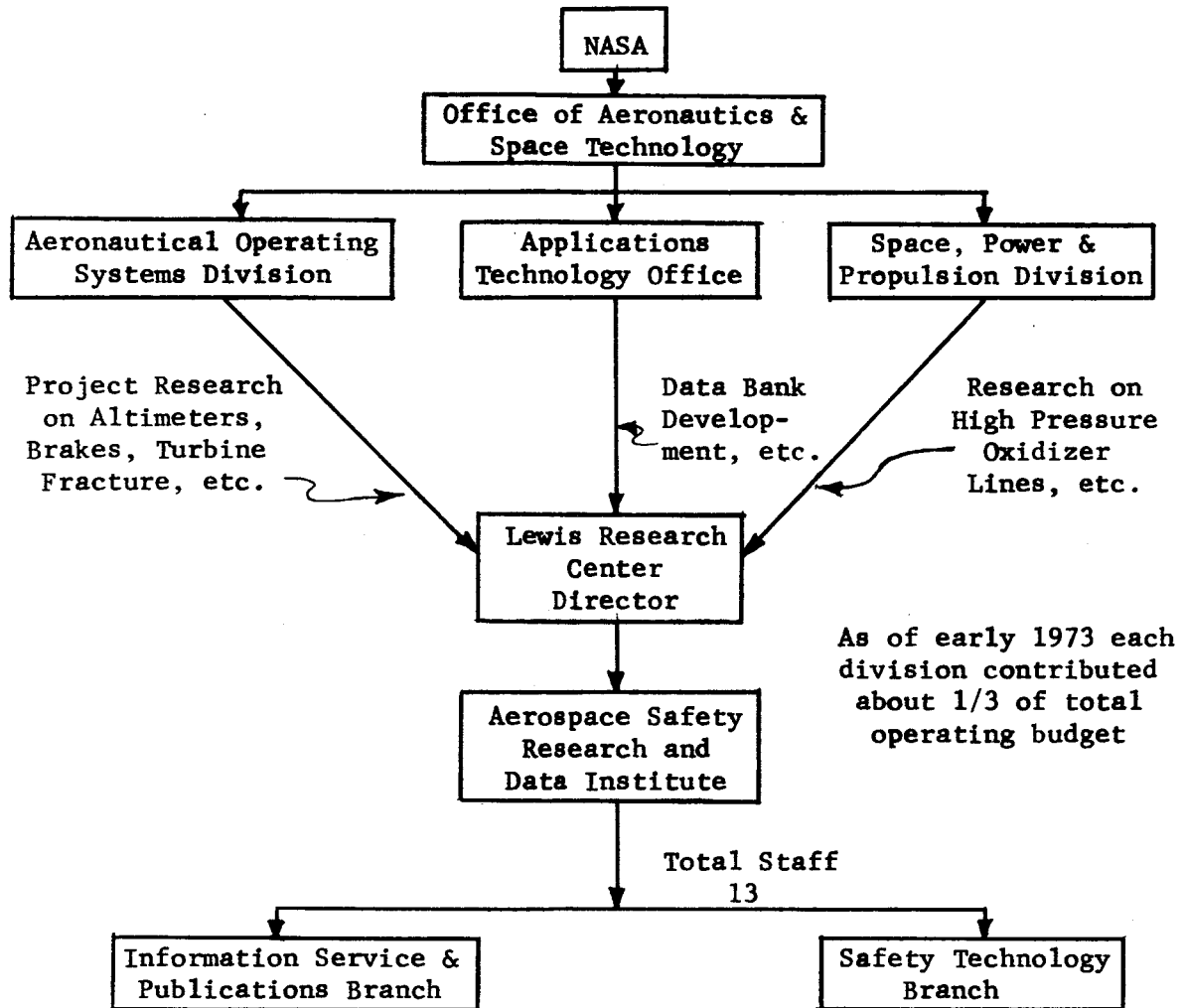
Figure 3. ASRDI Funding Flow and Organizational Relationships

D. TRANSFER OF SAFETY INFORMATION

This section will examine the elements of a transfer system, i.e. the mechanics of the actual transfer process. A systematic approach for transferring new technologies or information from point of origin to potential points of use is diagramed in Figure 4, page 67.

There has been an immense output of literature on the subject of information transfer in the past six or seven years. Accordingly, the process given below is not original here, but is a synthesis of the technology transfer process.* There are seven elements which are crucial to the mechanics of the process of information transfer. These elements are explained, and ASRDI is then examined in terms of each.

1. Information Organization

The first step in the information transfer process is to identify, evaluate, characterize, and catalogue information resources, both internal and external. This would involve systematic acquisition of knowledge in the form of documents, books, tapes, and research reports into a centralized data bank. A register of safety experts in various fields both inside and outside the institution might be a key input. The

---

*For further information on technology transfer see: Raymond A. Bauer. "Second Order Consequences," a methodological essay on the impact of technology. Ch. 10. The Transfer of Space Technology, MIT Press, 1969; R. J. Lesher and G. J. Howick. Assessing Technology Transfer. NASA SP-5067, Washington, D. C.: U. S. Government Printing Office, 1966; Richard N. Foster. "Organize for Technology Transfer," Harvard Business Review, Nov/ Dec. 1971, pp. 110-120; and George Steiner. "Improving the Transfer of Government Sponsored Technology," Business Horizons, Fall 1966, pp. 55-62.

```
                    ┌─────────────────────┐
                    │   Information Base   │
                    │ (Updated constantly │
                    │  through research & │
                    │     other means)    │
                    └─────────────────────┘
                        │             │
                        ▼             ▼
              ┌──────────────┐  ┌──────────────┐
              │  Identifying │  │  Identifying │
              │ Technologies │  │  Problems &  │
              │ for Transfer │  │ Needs of Users│
              └──────────────┘  └──────────────┘
                        │             │
                        ▼             ▼
              ┌────────────────────────────┐
              │   Matching Alternative     │
              │ Approaches, Technologies   │
              │        and Needs           │
              ├────────────────────────────┤
              │   Evaluation & Selection   │
              └────────────────────────────┘
                           │
                           ▼
                 ┌──────────────────┐
                 │  Dissemination   │
                 │     to User      │
                 └──────────────────┘
                           │
                           ▼
                 ┌──────────────────┐
                 │  Successful or   │
                 │  Unsuccessful    │
                 │    Transfer      │
                 └──────────────────┘
                           │
                           ▼
              ┌────────────────────────────┐
              │  Feedback      Analysis    │
              │         Planning           │
              └────────────────────────────┘
```
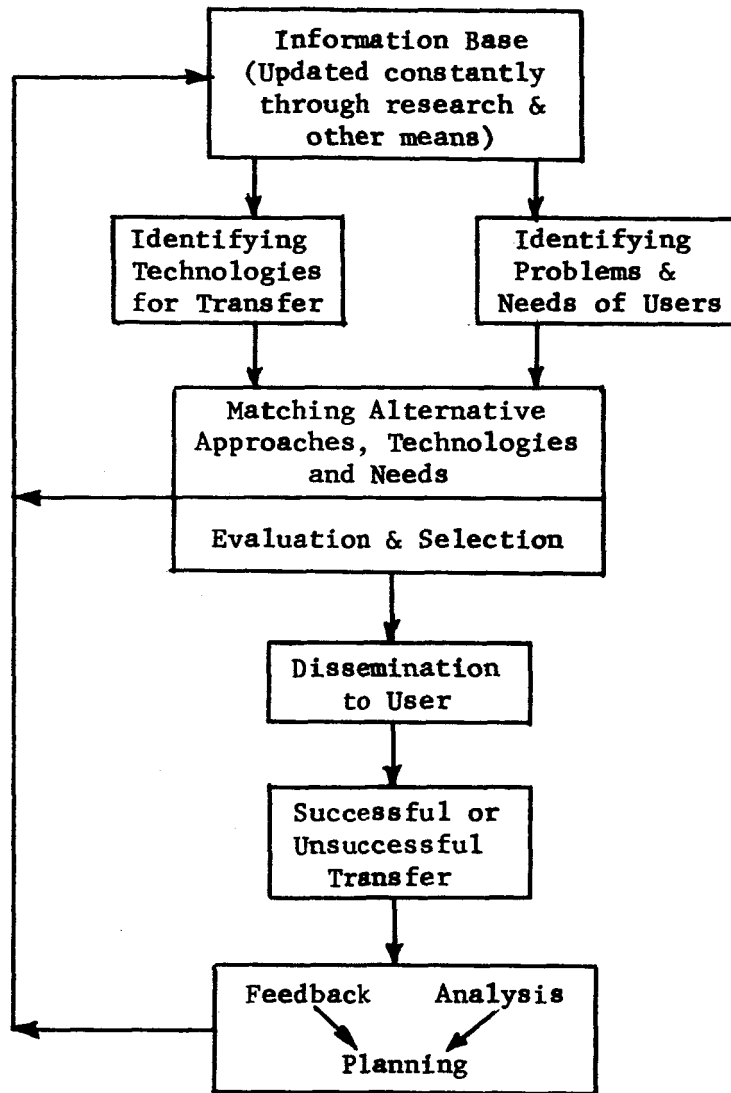
Figure 4. Steps Involved in the Transfer of

Safety Information*

* Adapted from Richard N. Foster, "Organize for Technology
  Transfer," Harvard Business Review, Nov-Dec. 1971, p. 112.

acquisition for the data bank or library must be made by technically competent people, and the information employed must be screened for relevancy (to users) and catalogued for easy access. In the case of the "register of experts" (Directory of Workers in the Fire Field prepared by ASRDI), it is absolutely essential that it be constantly updated.

In accordance with its mandate, ASRDI has established a library and a data bank. The data bank is an interactive, on-line grid system for storing and retrieving information for ready access. Although the original idea was to establish a large system, ASRDI has now scaled down the scope of the information storage and retrieval system. In addition to the above system, the more general NASA/RECON System which is used by ASRDI stores a vast quantity of published and unpublished safety information. Through the use of key words, a user can have immediate, refined information on any topic of interest.

Other safety centers have helped to supply safety knowledge which has been screened and incorporated into the data bank. ASRDI has also derived information from contractors and incorporated this into the data bank. Lockheed and General Electric, among others, have supplied safety information which ASRDI has been able to persuade these companies to share and for which ASRDI has publicly acknowledged receipt. Some of these volunteered reports have been exhaustive and excellent. This was a particularly useful accomplishment on the part of ASRDI as companies are usually secretive about trade information. In this connection, questions were raised by some members from other centers as to whether

ASRDI could afford to keep all this information or whether they should simply direct users to the proper source instead of storing it. We believe that their screening the information and storing it where other NASA users can have ready access to it is definitely more effective and efficient.

Requests from users, of course, have also helped shape the data bank. Requests concerning oxygen-cryogenic fluids have been among the main items requested. In addition, ASRDI has been compiling a register of experts and organizations with expertise in particular safety areas through a contract given to Martin Marietta and SDC Corporation, e.g., the Directory of Fire Workers mentioned earlier. Using this register of experts, ASRDI can directly facilitate contacts between users and experts in cases where they do not have in-house expertise.

In gathering information for input, ASRDI sifts, reviews, screens, evaluates, abstracts, indexes, and validates much of the material. For example, in the preparation of the oxygen/cryogenic series, about 1600 documents were screened, evaluated, and abstracted. In this case, there were some data inputs which would be worthy of future study. Unavoidably, NASA personnel with varied backgrounds evaluated information and used differing judgments in indexing, evaluating, and screening inputs which created some problems for the users of the index.

Storage space has been a problem for ASRDI. It was probably over-optimistic in the initial setup of the present system. Too many combination words were used, leading to frustrations on the part of some of the

users. There were consequent delays and set-backs before a fully opera-
tional system evolved.

In the data bank, ASRDI has information connected with aerospace
but useful to many other people and various industries, e.g., data on
tire skids, brakes, etc. Various industrial users have contacted ASRDI
for information on these matters, and responding to these requests takes
up a great amount of time, money, and storage space. The crucial question
is whether ASRDI can do this in view of its cost and other priorities.
We feel that this service should be carried out on a continuing basis,
but some method should be devised by which non-NASA users can be charged
for services rendered.

We believe that the present information organization in ASRDI, al-
though excellent, is not optimally founded on user needs and priorities,
or on NASA top management's conceptions of needs, priorities, and expecta-
tions. Evidence for the statement comes from other centers, users, and
management personnel who have said they have not been fully satisfied by
the type of information provided by ASRDI. Specifically, some pointed
out the fact that ASRDI did not have anything in the data bank on acci-
dent investigations or accident incident reports and therefore do not
know the specific areas where program/project centers are being constantly
hurt. Only if ASRDI has such a data bank on accidents, etc., can they
analyze patterns and see gaps in areas where improvements are required,
or if information exists to have it transferred to the right people in
these areas to prevent recurrence of these accidents.

We realize that it is indeed a difficult job to build an information base to satisfy the needs of various groups. However, if the organization is to provide meaningful information it must reflect and be built on user needs and NASA Program/Project priorities. It must provide information of a type and in a form which is assimilable in existing design processes.

2. Identifying Problems and Needs

After information is evaluated and organized, steps to utilize this information actively must be found if the information is to be a useful resource and not just a stagnant pool. This makes it necessary to identify where existing knowledge can be used. Who should be responsible for this function of recognizing need? Should it be a) the technological originator, in this case ASRDI? b) the user, which in this case could be other NASA Safety Centers or the aerospace industry? or c) a third-party catalyst? Based on past experience, neither the technological originator nor the user has adequately performed this function of transfer. The technological originator is too busy with his research. As for the user, Calvin Mooers,* one of the pioneers in information systems, has pointed out that an information system will tend not to be used whenever it is more painful or troublesome for a user to have information than for him not to have it.

---

* Mooers, Calvin N. Mooers' Law, or why some retrieval systems are used and others are not, in Zator Technical Bulletin (136), December 1959, p. 1.

While ASRDI has been active in identifying problems and needs for research, it has not been active in identifying dissemination techniques. This gap exists because as technological information originators, ASRDI is more research-oriented, rather than problem-finding and dissemination-oriented. With the present limited staffing and funding, we believe that ASRDI cannot perform the additional function of identifying dissemination problems and needs.

In addition, no proper channels appear to exist for systematic problem identification or the accumulation of accident/incident reports concerning flight systems. Likewise, no proper channels appear to exist for transferring safety knowledge from flight to ground systems, except through STAR, AIAA, etc. R & D flight personnel do not appear to interact with non-R & D flight personnel. If the channels exist they do not appear to be used. We feel a more systematic transfer of problems and information should be developed from flight systems to ASRDI and then on to non-flight systems.

3. Matching, Evaluation, Selection, and Generation

Having identified and/or defined the recognized or potential need, information specialists must search the information base and identify technologies that could be applied to the recognized need, keeping in mind the sophistication of the user. It is, however, essential that the technical personnel, as a source of information, provide sufficient background information to convey an understanding of the operational aspects of the problem. If the user approaches ASRDI with a problem, the

important characteristics of the problem should be clearly spelled out to the information specialists. Where technology or knowledge suitable to the user does not exist, ASRDI has to design a project (in-house research), or contract it out. The latter method, although more costly in terms of time and money, is definitely more effective because it is a more specific form of technology transfer. In the simplest case of information transfer, however, what is already known is channeled to the needs of the users -- what some people have called solutions seeking problems rather than vice versa.

The next step in the transfer process is to evaluate and select among the alternatives the best method or technology in terms of costs and benefits, adaptability, etc. In the case of a specific recognized need, more than one applicable technology may be available. In the case of a potential need for which technology does not exist, in-house or contract research can be initiated. The more specific and narrow the technology the easier it is to select and transfer; conversely, the broader the technology, the harder it is to effect transfer. A distinction could also be made between vertical transfer, the progression from science to technology to product, and horizontal transfer, the adaptation and modification of technology from one application to another, even though wholly unrelated to the first. The evaluation and selection process involves ASRDI in the following:

a. Institutional Sources: libraries, laboratories, universities, information centers, professional societies, organizations, and groups.

b. Bibliographic Materials: books, journals, reports, patents, standards, and guides which may lead to other sources. Other sources would be data tapes and computerized tape libraries.

c. Experts: individuals in ASRDI or outside who have specialized knowledge or know how to find it.

ASRDI's own small system needs additional information specialists knowledgeable not only about in-house resources but also outside information sources which may even supplant some of their own services and systems. These information specialists would perform a valuable function as intermediaries between the available sources and ultimate users of information. They would also perform a useful function by comparing the coverage of competing services and avoiding costly duplication. As an example, if the R & D centers already had information on some problem, then there would be no point in adding the same information to the ASRDI library, except to identify the source.

In examining sources for making the information-user match, the user's sophistication should always be kept in mind: his needs, his cost in obtaining the information, and any specific problems that he may have such as language, legal problems, etc.

There are many areas, however, where knowledge does not exist. The specific safety questions may not have been asked before, or if asked, no answer has ever been obtained. Reports indicate that ASRDI gets many questions for which the answers cannot be pulled out of any file. In such cases, ASRDI has to initiate research. A few problem areas where ASRDI

has either been actively involved or has initiated such research are:
a) safety criteria for propellant safety hazard evaluation, b) rotor
burst, c) brake systems, and d) aircraft and spacecraft lightning
hazards. In such areas it is essential that ASRDI not only conduct on-
going research, but also anticipate safety problems. Forward research
obviates the necessity of pushing the panic button at the last minute
and is more economical.

Most of the ASRDI-initiated research is now contracted out to com-
panies and universities, but ASRDI directs the broad course of investiga-
tion. Though very little of the work is done in-house, they comment and
advise on the progress. Under the present setup, commenting, consulting,
advising, abstracting, and indexing leave very little time to do anything
else. These responsibilities, in conjunction with the research orienta-
tion of the staff, effectively block the aggressive matching and dissemina-
tion of safety information.

After the matching process, ASRDI must also make sure that the quality
and depth of the information given is what the user needs, making whatever
modifications or adaptations are necessary for easy assimilation. The
more specific the technology, the easier it is to transfer and for the
user to assimilate; the broader and more complex the technology, the harder
it is to transfer and to satisfy the user.

Among the many criticisms that have been leveled at ASRDI by user
organizations is that ASRDI has been too slow in responding to requests.
But in many cases, the problem has been stated vaguely or has been ill-

defined by the user. If the end use for information is not made clear, then ASRDI has difficulty designing an effective answer. Poorly defined question and answer exchanges may provide some information but the initial vagueness does not help in arriving at a meaningful solution, and this leads to frustration on the part of users. Again, many of the requests require prolonged research; obviously, answers to questions which require research do not come quickly.

4. Dissemination and Communication

The phase of dissemination and communication is one of the most important elements of the entire transfer process. In the case of the broader and more generalized transfer not actively involving the user, safety technology cannot be handed down to the user as a tangible transfer item, but can usually be transferred by the following conventional means:

> Talks and Lectures by knowledgeable people in the area
>
> Seminars, Meetings, and Personal Contacts
>
> Consulting and Research Reports

When the originator or catalyst transmits technology in any of these modes, it is termed the active form of dissemination. In contrast, the passive forms of dissemination involves the seeker or user finding the knowledge or technology that he wants through:

> Technical or other publications
>
> Computerized data banks
>
> Tape banks
>
> Regional dissemination centers

Some of these information transfer methods are complex and time consuming, but new modes of dissemination are currently being developed to make the transfer process more efficient.

Most of ASRDI's knowledge has been disseminated in conventional ways. As an example, in the accumulation and transfer of oxygen data, ASRDI personnel fully used all the steps of active dissemination. Key personnel attended cryogenic meetings with industry personnel, contractors, suppliers, and academicians. ASRDI was able to get lists of safety personnel involved in cryogenic operations and then sent these individuals exhaustive reports on the handling and transportation of cryogenic materials. Through their interaction with various Government agencies like the DOT, ICC, and NBS, ASRDI personnel were able to pass on this valuable information at almost no cost. All relevant NASA safety personnel received copies of the reports. In our opinion this was one of ASRDI's best efforts at information dissemination and an excellent case of successful transfer.

In the dissemination of other kinds of safety information to the aerospace industry, universities, etc., ASRDI has utilized STAR and AIAA. ASRDI hopes that such information will be disseminated through these media to users. There is actually a two-step dissemination process at work here which uses both direct transfer to users and general transfer through professional journals. ASRDI has also approached NASA's T.U. personnel directly to disseminate safety knowledge through T.U. briefs which have a wide audience. With the same objective in mind, they have

issued some of the NBS Boulder reports through the NASA SP system.

ASRDI has been able to reach the in-house NASA safety personnel through internal directories and STAR reports. They also have utilized the accident-incident preventive action system reports and safety summary reports, which have been disseminated to the field through various meetings and the usual channels described above. While ASRDI cannot forecast accidents, they hope that through these reports, which are essentially "experience retention," the generic nature and causes of accidents can be discerned to prevent accidents. ASRDI must periodically find out how useful these reports are and what can be done to improve information transfer.

ASRDI has made the dissemination of safety information through the computerized data bank as easy as possible by using simple key-word indexing to retrieve information. Some users have had problems with the system, but to solve such problems ASRDI personnel have always been accessible to clarify matters by telephone. In addition, ASRDI has two NASA RECON terminals where in-house personnel can directly query the system and get safety-related information. Attempts have also been made to disseminate knowledge through movies and other forms of multimedia presentation. ASRDI personnel believe that these transfer media forms offer great potential and should be expanded.

Most of ASRDI's safety information users have been systems and design engineers, operational personnel, and scientists. ASRDI has also disseminated knowledge to certain non-technical groups, but this has been minimal. Specific requests have usually been made at meetings

where ASRDI has interfaced with various groups. However, ASRDI has been

very careful in what they divulge at these meetings because they do not

want to be in the position of becoming a telephone answering service;

they get innumerable calls from various sources requesting information

sometimes already published in Tech Briefs and other sources. Users

often do not take the trouble of finding out whether information is al-

ready available in published sources or their own data banks, but use

ASRDI as an information answering service. Such redundancy would in-

crease by becoming too visible, since ASRDI is not geared for mass service

operation, but perhaps they should be. One further point is that external

(non-NASA) requests for information are routinely handled without ASRDI

being compensated for the time spent.

5. Barriers

The process of technology transfer can be thwarted by several

barriers, some of which are:

> The "not in-house factor" -- a built-in resistance to
> ideas generated from outside the organization.
>
> A natural resistance to any change -- personal inertia.
>
> Absence of mechanisms within organizations to transfer
> knowledge.
>
> Failure of internal communications, poor communications,
> and delays.
>
> Problems in screening, cataloging, updating, etc. -- too
> much obsolescent information.
>
> Difficulty in assimilating needs of the user, and level
> of user's sophistication, language, etc.

Time, money, costs, and personnel problems.

Patent, licensing, and allied legal problems.

Concentration on the short-run rather than the long-run.

Poor visibility of the source.

Lack of confidence in source.

Lack of responsiveness to users.

The transmission of information is impeded not only by physical barriers but also by intellectual resistance and the lack of efficient channels for the transmission of information. Barriers exist within the management of an agency, in its personnel, and in potential users. A systematic elimination of these barriers is essential if the transfer process is to be smooth.

An attitude of "we have discovered this information, we have identified it, and if someone else wants it he can bome and get it from us" on the part of the source can be as detrimental and damaging to the transfer process as the attitude of "if it is not invented here it is not worth having," on the part of the user.

The Syracuse University research team had an opportunity to look at these various barriers on their visits to various centers. Certain personnel from other safety centers made the comment that much safety work is being done beside that at their own facility, and thus asked, "Why this duplication; why call ASRDI?"

Although ASRDI does have some visibility, it is somewhat limited, and it has purposely kept a low profile. What little visibility does

exist has been attained by getting their names on reports, STAR, AIAA,
Tech Briefs, and by interfacing at interagency meetings. ASRDI has had
to adopt this low profile because, as stated above, they do not want to
be swamped with requests with existing manpower limitations.

We have to some extent discussed the question of resources -- money
and staffing. Lack of funds for travel is especially detrimental to
the transfer process. This is important because frequent personal inter-
action is one of the most effective means of unearthing problems and
transmitting technical information and technology. Information and
technology flow not on the basis of formal communications systems alone
but very effectively through personal interaction. Improving the quality
of a particular information source will not lead to increased use as
much as accessibility of the source. The potential user such as an
engineer in NASA requiring technical information may tend to downgrade
pieces of literature or articles because they are outside his coding
system but will place more faith in personal contacts.

Providing travel money alone without providing the necessary back-
up staff to meet the increased demand that will follow is futile. The
existing and the additional staff must also be challenged and motivated
to perform the transfer function.

Some NASA personnel have commented that some of the information
provided by ASRDI does not meet their needs, and they fault the narrow-
ness of interest among ASRDI's scientists and engineers. This criticism
is puzzling because others have criticized ASRDI for just the opposite --

too broad an interest. It is indeed no easy task to satisfy the needs
of diverse groups, and one of the major gaps is an understanding of
this human factor in the technology transfer process.

6. Organization and Funding

Organizational management skills and experience are essential in
the transfer of technology. Effective transfer cannot take place with-
out an organization and management structure in which management brings
skills, experience, and resources together to respond to systems problems.
The group which collects and disseminates information must have authority
to do so, or their work is more difficult.

NASA Safety Centers

NASA safety organizations are located at Headquarters and at the
field centers. Each center has a safety office with safety engineers
and other safety staff to perform the complex safety functions required.
ASRDI interfaces with all these centers, as well as other NASA panels
and offices like ASAP and the Technology Utilization Division. ASRDI
is currently involved in two or three aerospace problems with the Tech-
nology Utilization Division. Other NASA organizations with which ASRDI
interfaces are:

      NASA Spacecraft Fire Hazards Steering Committee

      Shuttle Safety Operations and Maintenance Working Group

      OMSF Space Shuttle Safety Advisory Panel

      NASA Research and Technology Advisory Subcommittee on
      Aircraft Operating Problems

Space Base Nuclear Systems Safety Steering Committee

JANNAF Hazards Working Group (Joint Army, Navy, NASA
Air Force)

ASRDI thinks of itself as a supportive resource rather than an opera-
tion resource. The relationship with other NASA Centers, flight and non-
flight, is thus not regular or formal; rather, it tends to be more trans-
ient and lateral. Since there are no regularized or formal reporting
relationships with other centers, communication also tends to be some-
what unsystematic and sporadic. In interfacing with these NASA Safety
Centers, ASRDI personnel do not get into safety on a day-to-day basis,
nor do they tell other safety groups how to manage their safety opera-
tions; ASRDI does not want to get into configuration management. They
can advise where there are specific problems or where lines of communica-
tions have been opened, but it is not their function to catch configura-
tion errors and the like on a routine basis.

Links with Other Government Agencies and Industries

ASRDI also interacts with other Government agencies like OSHA, DOT,
ICC, Fire Information Users Standing Committee (NBS), Government Inter-
agency Committee for Mechanical Failures and Prevention, Government
Agency Seating Working Committee, and Compressed Gas Association's
Cryogenic and Low Temperature Committee. ASRDI establishes contacts,
exchanges information and advice, prepares guidelines, and identifies
problem areas requiring research through these committees. There is a
great deal of two-way information flow here.

While ASRDI has a fairly good record of in-house, interagency/industry cooperation, room exists for innovative possibilities for further coopera- tion in research development and transfer of safety knowledge. Perhaps what ASRDI needs is to critically examine its work for NASA Centers and other Government agencies with a view toward optimally relating its in- ternal capabilities to external information needs. ASRDI should broaden its policy of interagency cooperation to accommodate a broad spectrum of needs. It would be useful for ASRDI to exchange personnel with other agencies, provide on-the-job training for personnel from other agencies, and even investigate the possibilities of special joint projects. As stated above, the most economical and effective way of transferring safety knowledge is through the interaction of personnel.

Another point the Syracuse University research group looked into was whether ASRDI could do a better job of collecting and disseminating knowledge if it were given some sort of regulatory status inside NASA. At present it is a staff department with no line authority to enforce its requirements. ASRDI personnel are strongly against the idea of being a regulatory agency. We concur with them that an advisor's and policeman's role do not go well together. A regulatory role for ASRDI would restrict its interfacing with other centers, agencies, and industries, while data collection and dissemination would become more difficult. ASRDI would be closed out of many places and information sources.

Formalization of ASRDI and Center Contacts

For the most part, ASRDI has been viewed by the other NASA Centers

as primarily a Lewis-oriented operation with limited relevance to their own organizations. A NASA Management Instruction was never written for ASRDI, defining relations with other Safety Centers and Headquarters, i.e., ASRDI's mission was never "formally" established. We feel that if an ASRDI Management Instruction were clearly written and communicated, the other Centers would more fully understand the ASRDI mission and would be more prone to utilize its services. Although we realize that the issuance of an Instruction Sheet per se will not solve all of ASRDI's problems, it would at least provide some direction and purpose.

The Syracuse University research team raised the question of the feasibility of ASRDI establishing a single formal contact person at any given Center so that interfacing could be improved and the communications flow could be more systematic. ASRDI personnel felt that on specific technical issues it was better to get directly involved with the person dealing with a particular safety issue or problem. ASRDI personnel alluded to requests from individuals in other Centers which bypassed the Center's own safety organizations. It was not because the individuals wanted to bypass their own Center safety organization, but that often the center safety office was not directly involved, interested, or concerned with the given problem and this speeded up communication. But ASRDI personnel did feel that if the problem was of a general nature and one did not know the individuals at the other end, then a formal contact person would help ease communications.

Systems Safety

Organizational interfacing on Systems Safety problems raises additional difficulties. Systems Safety is a complex and complicated discipline. It is often necessary for ASRDI to interface with project groups who are using Systems Safety concepts, and as part of this interfacing ASRDI should participate in the key safety committees at early design stages. They should ask the right questions at the right time and should have checklists and statistical data in order to help make Systems Safety more efficient.

The problem, however, is that the personnel from ASRDI who sometimes sit on and advise these committees have to be knowledgeable about Systems Safety techniques as well as pertinent technical areas. ASRDI has specialization in about 16 areas, but Systems Safety itself is becoming so specialized and complicated that it is almost impossible for individuals to keep up with both the latest in Systems Safety and a particular science. Thus, ASRDI personnel realize that it is impossible to contribute to every committee, and as a consequence, ASRDI must be selective in determining priorities. This selectivity becomes a problem when other centers perceive ASRDI as able to provide help in all areas, however specialized, and are disappointed if ASRDI is unable to supply men or information.

Need for a Unified Funding Source

Another ASRDI problem area is that of funding. As stated in Part C of this Section, ASRDI's funds come from the following agencies:

1. Aeronautical Operating Systems Division

2. Applications Technology Office

3. Space Propulsion and Power Division

4. Aerospace Industry (miscellaneous work)

Much of ASRDI's funds are provided for specific projects of interest to the particular funding agency. Because funds do not come from one source such as the NASA Headquarters SR&QA Office, it is quite natural for questions of priorities, conflicts, and questions of responsiveness to develop when ASRDI derives its funding from multiple sources. Conflicts, if any, are informally worked out.

Negotiating with three or four groups for monetary support for projects is also tedious and time consuming. ASRDI personnel are never sure where their funding will originate and when it will terminate. Uncertainty impeded transfer and forward planning while certainly putting a strain on effective functioning.

Need to Shift ASRDI to Washington

One other question that engaged the Syracuse University team's attention was whether ASRDI as an organization should be shifted out of the Lewis Research Center to Headquarters. The original placement at Lewis has been questioned by others. Shifting ASRDI to Headquarters would be helpful in changing people's perception of and attention toward ASRDI as having Headquarters status. Visibility for ASRDI would be definitely improved. Once users perceive this new relationship, the input of information to ASRDI would probably improve. ASRDI might be called upon

to interact more, which could help the transfer process. Some other
personnel, however, felt that ASRDI was better left at Lewis and that
this was in line with NASA's overall policy of limiting Headquarter's
control and letting organizations such as ASRDI fend for themselves in
the competitive system. An answer to this question can only be made
after evaluating the pros and cons of the idea of a move to Washington
Headquarters.

There would be several advantages to such a move. Administrative
and public visibility would improve. As with other major program offices
in NASA, not only would other specialized NASA talents become accessible
to ASRDI, but ASRDI, too, would become more accessible to others, being
more visible and more in the focus of the dissemination of safety knowl-
edge. Unified funding and centralized management could provide a NASA-
wide coordination of priorities and better control. A move to Head-
quarters would not replace or conflict with any existing organization
in SR&QA at Headquarters. A move could centralize information on safety
problems for both manned and unmanned aerospace work. The physical
proximity to other agencies interested in a host of safety-related prob-
lems could be enhanced by the move. With the cooperation of an effective
Safety Applications Team, the move would help match NASA skills to ap-
plication areas where no active matching efforts have previously been
made. There would be a systematic activity instead of an incidental
one; looking for opportunities instead of responding to external requests.

The disadvantages of moving ASRDI to Headquarters must be considered. Commitments of the Office of Systems Safety at Headquarters, both present and anticipated, appear to exceed available manpower and dollars. Thus, it would be difficult to accommodate ASRDI in that office. The general nature of Headquarters' work might detract from ASRDI's concentration on their primary mission of research and dissemination. Existing safety offices at Centers might not fully cooperate with ASRDI and provide support since they might see ASRDI interferring with their freedom and autonomy. The extensive Lewis Research facilities would no longer be readily available to ASRDI.

Need for a Change in Staff Orientation

As stated above, ASRDI's staff is research-oriented. If ASRDI is to become a good dissemination operation, then the staff mix must change to include multidisciplinary people skilled in both engineering and external communications. In addition, they need more "travel missionaries," translators, and the like. The present information staff has done some work in such areas as cryogenics and rotor burst, but has been inhibited from doing more because of the lack of more information specialists.

7. Planning

There must be constant comprehensive planning to see that transfer is systematic and ongoing. Effective planning must not only look ahead to see changes which may impede the transfer process, but also to see how the present process can be improved. Good and bad examples of transfer should be studied and an attempt made to measure transfer and its

effects. A systematic feedback mechanism and continuing analysis of the entire process is essential.

Systematic planning has not been done in the past at ASRDI for various reasons, but primarily because most of its operations have been short-range and problem-oriented, carried out on an ad hoc basis. Whenever requests or problems come in, ASRDI has tried to provide the information if available, and if not, has had to assemble it or initiate research. Present programs were not fully planned in advance. For example, subsequent top management directives changed the original Liquified Natural Gas study to other priorities and oriented efforts in another direction. Aside from these directives from above, multiple source funding also tends to inhibit comprehensive long-range planning.

Although a broad plan and policy is lacking, ASRDI currently has an impressive list of projects, many of them potentially promising and important. It would be extremely useful to adopt a more formal planning system to provide integrative management. We believe they should ask the following questions: Where is ASRDI now? What is their mission? Which safety areas are of most concern? What should they be planning in terms of safety information transfer and research in the future?

An additional element in the planning area is marketing. ASRDI should strongly market and advertise its products and services. This could be the key to success in the future.

E. RECOMMENDATIONS

The recommendations that follow are numbered from 1 to 7 to correspond broadly to the seven elements discussed in the preceding pages.

1. Information Organization

We recommend that ASRDI make a concentrated effort to obtain current information on the needs and requirements of various users of safety information at all levels within NASA. Such a study should extend to Headquarters, safety management, institution and program management, field installation management, field safety management, functional management, contractors, and all appropriate personnel. A telephone or mail survey should seek to determine "interest profiles" including:

What types of safety information do you need?

What types of safety information do you regularly get?

What types of special safety studies do you periodically request?

What types of service or safety information would you like to get which you are not getting now?

Would you want it daily, weekly, monthly, or only on request?

What specific topics in safety would you like to be kept informed of?

What type of safety data analysis programs would you like to have made available?

What do you think would be the most helpful improvements that could be made in the present system?

As part of the survey, Program/Project Management's conception of just how safety information can be organized should be sought by ASRDI in as

explicit terms as possible. The results of the survey would be the basis

for developing a plan for improving the ASRDI information organization.

Program/Project personnel and other NASA Centers must now seek in-

formation on various matters from ASRDI. As with any other system, a

certain amount of dissatisfaction is to be expected. However, users must

be held responsible for facilitating the operation of the system, and

should not put all the responsibility on ASRDI. The tendency on the part

of users has been to stop asking if they have been dissatisfied once in

their attempts to get information. Constant interaction and pushing on

the users' part can help build a better system.

The Syracuse University group did not go into the question of what

kinds of safety information were needed by NASA program/project Centers

and thus what ASRDI should be supplying. Such a study would have extended

us beyond our objective. The kind of safety information needed can be

better determined by ASRDI.

2. Identifying Problems and Needs

A Safety Application Team should be established to define problems,

needs and areas of potential improvements. NASA has in the past made use

of application teams for problem identification and problem solution

methodology. One of the first such application teams was the Biomedical

Application team whose success spawned the establishment of several tech-

nology application teams. The function of these teams is to act as

catalysts bringing together the user needs with the expertise within

NASA. Most often they perform a "broker" function by providing the link

between the technological source and the user while not depending on the initiative of the originator or user alone. The rationale for establishing these teams was that mechanisms and systems designed in support of specific project areas of space exploration, manned or unmanned, could be helpful to other project areas. A similar Safety Application Team should not be based at universities or other non-profit institutions operating under contract to NASA; we recommend that it be a new unit within ASRDI. The team should of necessity be multidisciplinary, and should perform the intermediary or broker role which ASRDI performs now.

The Safety Application Team could meet with other NASA Safety Centers and Governmental agencies to identify and obtain descriptions of specific operational problems which could be solved by the application of existing technology. The Team could prepare concise problem statements highlighting the important characteristics of certain problems, with sufficient background information to convey an understanding of operational aspects.

One important function of a SAT would be to develop a more formalized approach to the collection, documentation, and analysis of accidents/ incidents to facilitate the identification of patterns of problems and needs.

The SAT team could be one of ASRDI's more interesting, ambitious, and potentially effective approaches to technology transfer; it contains a potential element of aggressive entrepreneurship (as much as ASRDI wants or feels it can allow) for effective transfer.

3. Matching, Evaluation, Selection and Generation

It would be well to distinguish information matching on two different bases: a) general needs, and b) individual needs. For general needs one could tap the data bank immediately for answers. For specific individual needs where a great deal of precise information is required, ASRDI can contribute in a variety of ways with a concerted effort if they are given sufficient background by the user and if they have the manpower to reply in depth. A framework for answering specific and unique requests would include:

a. Give the user all available facts and information, not only prior work, but also current articles, bibliographies, state-of-the-art reports, as well as facts about reliable and unreliable findings.

b. Offer to help in researching and interpreting the ASRDI library facilities and other available data banks to gather additional ideas.

c. Fill the user in on what has not been done and recommend to the user that ASRDI could initiate further research if desired, with the reminder that it would take time.

d. Give additional information on all those persons currently working in the field in case the user wanted to contact them independently.

e. Give advice on where other facilities might be available to carry out the work.

f. Explain possible applications of the safety knowledge and benefits which could be achieved.

g. Give information on costs, if possible.

h. Give information on legal constraints, if possible.

i. Provide positive follow-up to assure that the user is satisfied.

4. <u>Dissemination and Communication</u>

Visibility for ASRDI and rapid dissemination of useful safety information go hand in hand. The most economical and effective way to disseminate information is through personal interaction at various meetings. ASRDI should be encouraged to broaden its policy of inter-agency cooperation and interfacing. They could use "travel missionaries" who would visit all Centers, industry, etc., disseminating information, determining needs and reporting back to ASRDI. This would generate more tasks for ASRDI and improve visibility. These "missionaries" could be a part of the SAT team suggested or some modification of it.

In addition, ASRDI should develop a "hot line" or an open telephone line and encourage people to call them with problems. Even the risk of becoming a telephone answering service we feel would be justified to open communications with various people and increase visibility. This "hot line" would be in keeping with ASRDI's image as a service organization of NASA.

All ASRDI publications are now part of the Regional Dissemination Centers, but computerized information is not. Such information could be made available through the RECON at the various Centers and would enable safety information to be disseminated to a wider audience, giving ASRDI more visibility where it is important. Any form of dissemination that affords wider visibility should be extensively pursued.

5. <u>Barriers</u>

Removal of barriers is a <u>sine qua non</u> for the smooth transfer of technology. Following the framework suggested above in item 3 for every

request would help. Lack of confidence in source and lack of responsiveness to users are barriers which can be easily removed by need-fulfilling, service-oriented actions.

A formalized contact person at various Centers whose duties should be well defined would make communications and transfer more systematic. Finally, removal of the fear of ASRDI "going out of existence" will help the transfer process.

6. Organization and Funding

ASRDI needs a strong and visible focus for its people and activities. Every possible means to achieve this must be provided for by the Headquarters Safety and Reliability and Quality Assurance Office through in-house papers (such as _Aware_), directives, etc.

A NASA Management Instruction Sheet should be issued formalizing ASRDI, delineating responsibilities, and defining relations with other safety Centers and Headquarters. In addition, the organizational interfacing as regards Systems Safety should be spelled out.

A single unified source of funding, out of NASA Safety Headquarters, should be arranged, which would help ASRDI plan better and operate more efficiently.

There is a strong case for shifting ASRDI out of Lewis, if not physically then at least organizationally, into the SR&QA Office at Headquarters where it will have better visibility and accessibility. The move would give Headquarters more coordination and control over

priorities and directions, and with the unified source of funding, could make the organization more effective.

A change in the staff mix would appear necessary to make ASRDI a more effective dissemination and transfer agency. Multidisciplinary personnel with engineering and communications background and perhaps translators should be added to the staff.

Lack of funds is a continuing problem. Some method by which non-NASA users (industry demands) can be charged for the information services rendered by ASRDI should be worked out to relieve the tight budget situation and eliminate casual and unnecessary requests.

7. Planning

A comprehensive plan should be developed detailing ASRDI's current capabilities and programs and what they want to be as an organization in the future. This analysis would provide an evaluation of capabilities, a projection of evolving problems and technical needs, and a basis for decisions. The environment ASRDI will be operating in should determine the directions and priorities which ASRDI should take. Among the various questions ASRDI should consider in designing their basic strategy are:

What will their offerings be -- safety information transfer or safety research, or what judicious mix?

What functions deserve priorities?

Who are their customers? Who should their customers be?

What kinds of services and information will users need? (A questionnaire along the lines suggested above could assist in identifying user needs.)

What evolving technologies may provide threats to
safety and what can ASRDI do to collect, analyze,
store, and disseminate information on these tech-
nologies? Who are the experts in these areas?

What channels or modes of dissemination will be
used?

What facilities will be needed?

Will the research be in-house or contracted out?
If both, what should the mix be?

What are their personnel requirements and what skills
are needed?

What kind of a total system must be established to
ensure the supply of timely information to potential
users?

Planning must also include the formalization of a feedback system
for further improvement. We recommend the use of a formalized procedure
in the form of a questionnaire asking for comments on whether the user,
general users, or specific problem-oriented users are satisfied with
the information provided and, if not, what was wanted and how could
service be improved. Reminders and follow-ups may be necessary, and
although replies are not usually forthcoming, whatever feedback ASRDI
obtains would be useful in improving the transfer process.

In planning for the management and transfer of safety information,
ASRDI should seek activities that rest on its strength and have a re-
assuring prospect of success. Momentum should be built from a series
of important successes like the oxygen/cryogenic series in which ASRDI
did an admirable job of planning, collecting, and disseminating informa-
tion.

Analysis of performance, which is tied with the feedback system and must be an ongoing, self-evaluation process within ASRDI, should consider the following on a yearly basis:

1. Number of clients

2. Number of searches/documents ordered

3. Number of transfers

4. Marketing performance (repeated use of services)

5. Response and reaction of users

6. Personal relations with users

7. Testimonials and case studies

8. Overall impact of ASRDI on the safety knowledge
   of user institutions

Without getting involved in a numbers game, we feel that a very objective quantitative and qualitative analysis can be conducted to clearly highlight year-to-year improvements.

To ensure that the basic functions are accomplished efficiently it is necessary that adequate controls be established. This requires constant monitoring of every one of the seven elements discussed on a continuing basis to determine discrepancies, deficiencies between planned and actual achievements, and suitable measures for corrective action.

Any organization that does not plan ahead, does not market its capabilities persuasively, and does not show consistent improvement in performance every year will lose its support; it will be thought of

as an organization existing only to serve its own ends. The only way
to assure a continuing position to improve safety is to remain associated
with the aspirations of projects, programs, top management, and the needs
of users.

APPENDIX A

SAFETY REQUIREMENTS AND DEFINITIONS

A. INTRODUCTION

It is impossible to appreciate the tremendous and never-ending tasks required in the management of safety at NASA without some understanding of certain interrelated factors. The reader who is quite familiar with NASA's programs, its organizational structure, its contracting practices, and the enormous complexity of its systems will immediately recognize that any assurance function that starts with the earliest design concept and ends only after the review of a completed mission must be terribly difficult. Such a reader might still be unaware of the innumerable details involved in the assurance of safety in a program or individual mission where any one of so many critical elements could each cause failure.

For those not completely familiar with safety problems in general and system safety in particular, this section of the report presents very briefly the terminology of safety, risk, and related factors in an attempt to provide a reference base and some perspective for the major chapters of this report.

B. FUNCTIONAL AREAS OF SAFETY

Program safety in NASA encompasses four broad functional areas:

1. Systems safety

2. Industrial safety

3. Aviation safety

4. Public safety

The overall goal of the safety program in NASA is to avoid loss of life, injury to people, damage to and loss of equipment/property. In addition, the safety program aims at instilling a sense of safety awareness in employees and contractors, evaluating plans, systems, designs and activities relating to overall safety, and finally, assuring that an organized and systematic approach is used to identify hazards to contribute to overall mission success.

To achieve these goals is indeed no ordinary task. Beside engineering or technical knowhow, expertise in overall program safety management requires a basic understanding of human resource management, plans, organization, communication, and adequate financing to motivate and train personnel to improve their job performance. While the main focus of this study is on system safety in NASA, it would be worthwhile to look at what these other functional areas are and how they relate to systems safety.

Industrial safety, in general, includes the many methods, disciplines, and procedures which assure protection of employees on a day-to-day basis.

With the enactment of the Occupational Safety and Health Act of 1970,
NASA has had to ensure that safe and healthy working conditions are
maintained. Industrial safety covers quite a broad range of activities
including:

1. Fire prevention and protection

2. Handling and storage of materials

3. Transportation safety

4. Pollution and waste disposal

5. Pesticide control

6. Medical and environmental health

7. Protective equipment

8. Radiation and noise safety

Aviation safety is one of the most important areas of the NASA safety
program. The prevention of flight-related accidents requires a safety
program that is quite broad in scope, covering all aspects of flying, ex-
perimental flying, routine administrative flying, and cargo safety.

Public safety is treated by NASA as an extension of system, industrial,
and aviation safety. NASA recognizes its responsibility to the public that
any hazards arising from the conduct of NASA activities be properly identi-
fied and eliminated or controlled within limits which protect public health,
safety, and property.

From the above, it is easy to see that overall program safety inter-
faces with all of NASA activities. For example, safety is critical in
manufacturing (fabrication, assembling, validation testing), operations

(test safety, pad safety, public safety, launch recovery), design (boosters, experiments), and logistics (packaging, transportation, handling, etc.). The overall program will definitely be cost effective and will minimize the loss of resources, increasing the probability of mission success in addition to providing greater national social acceptance. The safety program will also provide a storehouse of information and skills for use in future programs; it must, however, have full program management backing to be totally effective.
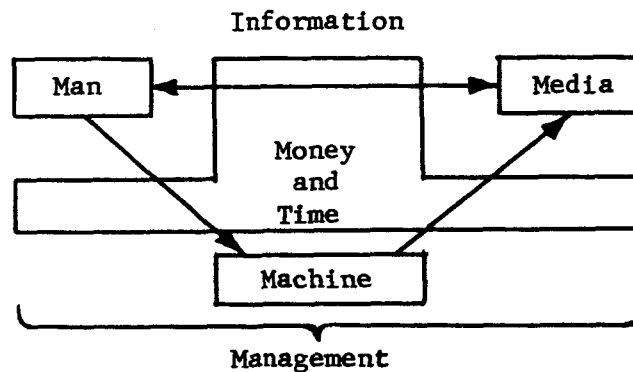
C. SYSTEMS SAFETY

In the last two decades, the increasing complexity of equipment and processes and the increasingly hazardous environment in which the equipment and processes operate has brought to the forefront a relatively new branch of engineering -- system safety engineering. Although pioneered and developed by the Air Force -- and later on by the Navy -- it is now used extensively not only by the Department of Defense but other Government agencies and, of late, by industry as well.

The National Aeronautics and Space Administration stepped up the usage of system safety in 1967 after the Apollo AS-204 fire. Until 1967, NASA's safety program was fragmented at best. The fire and the death of three astronauts changed all that and forced NASA to consider the systems aspect of safety in a way that was unmatched by any single impact in any organization.

As developed by the Air Force in the earlier stages, system safety was more of an engineering discipline than a safety management program. (The Air Force now has its own safety requirements published in a large Design handbook -- for which Norton A. F. Base is responsible -- as well as a Development Engineers Handbook.) NASA's great contribution was to pick up system safety engineering as it existed in 1967 and add "human safety" and its own management expertise to the system safety concept. NASA considered an understanding of "human behavior" to be as basic a requirement as the engineering principles involved.

System safety is essentially the integration of skills and resources specifically organized so as to achieve safety over all phases of a system's life cycle. It also involves "Methodical Hazard Identification and cost effective management application of hazard controls to attain acceptable safety throughout the systems life cycle."[*] System safety is also an analytical approach used to predict how a system can fail and to devise ways to avoid failure. The basic attitude in the whole concept must be one of questioning. As C. O. Miller, Director of the Bureau of Aviation Safety for the National Transportation Safety Board, states it, you must always ask, "What if?"

To show the interrelationships between man, machine, media, factors of accident causation and prevention together with time, cost, and information constraints in the real world, we reproduce below a sketch used by Mr. C. O. Miller.[**]

_____

*C. W. Childs, NASA Headquarters, "Industrial Accident Prevention Through Systems Safety," paper presented at The System Safety Symposium July 17, 1973, Denver, Colorado.

**C. O. Miller, "Why 'Systems Safety'?" Technology Review, Feb. 1971. p. 30.

Quoting Mr. Charles Childs* of the NASA Safety Reliability and

Quality Assurance Office, systems safety requires the following:

1. Survey of similar programs and projects -- historical safety data if any

2. The establishment of guidelines, constraints for operations, and also the scope of the system safety effort -- tradeoffs

3. Hazard analyses -- identifying sources and whether they are catastrophic, critical, marginal, negligible

4. Safety trade studies

5. Safety analysis reports

6. Change review analysis

7. Post flight/mission evaluation

The analyses, while mostly qualitative and deductive, are designed to

break the system into convenient subsystem elements and activities. The

techniques of analysis will differ in approach and depth depending on

the complexity of the system and the results to be obtained.

As to why a formal well-organized safety program is needed, NASA

states in its Safety Manual:**

1. The complexity of systems, subsystems and components under extreme and varying conditions of environment and application. The inherent complexity of the NASA flight hardware systems demands technical and analytical techniques of considerable sophistication in order to achieve problem identification and solution.

---

*Ibid.
**NASA Safety Manual, Vol. 1, Basic Safety Requirements, 1969, p. 3-3 and 4.

2. The need to fix considerable attention on the safety considerations arising out of total systems effects cannot be discovered when considering portions of the system independently.

3. The subtleties inherent in the dynamic characteristics of flight hardware systems.

4. The need to assure that the safety aspects of the mission under normal conditions and under mission failure conditions are adequate.

5. The need to assure that system safety measures at all steps leading up to, during and after the mission are adequate.

   It is much more effective for any aerospace system from the standpoint of program impact and costs in terms of both time and money, to allocate resources for the identification and reduction of hazards, than for accident investigation, corrective actions, lost effort and hardware replacement.

D. SYSTEMS SAFETY TERMINOLOGY

The field of Systems Safety is not without its terminological complications. An understanding of the meaning of certain terms is necessary to compare Systems Safety program objectives, activities, and management techniques at various other centers. We will, therefore, define the safety terms which are used in this report.

Safety and Systems Safety

NASA defines "Safety" and "Systems Safety" as follows:*

> Safety: Freedom from chance of injury or loss to personnel, equipment, or property.
>
> Systems Safety: The optimum degree of risk management within the constraints of operational effectiveness, time, and cost attained through the application of management and engineering principles throughout all phases of a program.

The Department of Defense in MIL-STD-882 defines the two terms as follows:**

> Safety: Freedom from those conditions that can cause injury or death to personnel, damage to or loss of equipment or property.
>
> Systems Safety: The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of systems safety management and engineering principles throughout all phases of a system's life cycle.

---

*Systems Safety Guidelines for Manned Space Flight Programs, Revised Preliminary Draft, Sept. 11, 1967, Office of Manned Space Flight, NASA, pp. 1-4, 1-5.

**Military Standard System Safety Program for Systems and Associated Sybsystems and Equipment—Requirements for, 15 July 69, p. 2.

The difference between the two definitions is in NASA's introduction of risk management, "risk" being defined as the chance of injury or loss to personnel, equipment or property. The definitions are similar to the extent that both of them recognize there are times in the program when some tradeoffs between the level of safety that could be reached and the increase in cost and time will have to be made in the interest of meeting mission requirements. Further, all definitions stress that Systems Safety is achieved by the use of engineering principles and management techniques throughout the entire life cycle of the system.

Systems Safety Engineering

Systems safety engineering is an element of systems engineering, involving the application of scientific and engineering principles for the timely identification of hazards and initiation of those actions necessary to prevent or control hazards within the system. It draws upon professional knowledge and specialized skills to specify, predict, and evaluate the safety of a system.

Systems Safety Management

Systems safety management is an element of program management which insures the accomplishment of Systems Safety tasks, including identification of the Systems Safety requirements: planning, organizing, and controlling those efforts which are directed toward achieving the safety goals; coordinating with other (system) program elements; and analyzing, reviewing and evaluating the program to insure effective and timely realization of the Systems Safety objectives.

Hazard Analysis

Hazard analysis, as summarized by Hammer,* is the investigation and evaluation of:

1. The interrelationships of primary, initiating, and contributory hazards that may be present

2. The circumstances, conditions, equipment, personnel, and other factors involved in safety of a product or the safety of the system and its operation

3. The means of avoiding or eliminating any specific hazard by use of suitable designs, procedures, processes, or material

4. The controls that may be required for possible hazards and the best methods for incorporating those controls in the product or system

5. The possible damaging effects resulting from lack or loss of control of any hazard that cannot be avoided or eliminated

6. The safeguards for preventing injury or damage if control of the hazard is lost

Preliminary Hazard Analysis

Hammer** points out that hazard analysis consists of making a study during concept planning or early development of a product/system to determine the hazards that could be present during operational use. The Preliminary Hazard Analysis helps establish the courses of action to be taken, its principal advantages being:

1. Its results may help develop the guidelines and criteria to be followed in product or system design.

---

*Willie Hammer, Handbook of Systems and Product Safety, 1972, p. 86.
**Ibid., p. 108.

2. Since it indicates the principal hazards as they are known when the product is first conceived, it can be used to initiate actions for their elimination, minimization, and control almost from the start.

3. It can be used to designate management and technical responsibilities for safety tasks and as a checklist to ensure their accomplishment.

4. It can indicate the information that must be reviewed in codes, specifications, standards, and other documents governing precautions and safeguards to be taken for each hazard.

Hazard analysis is of special importance where there is little similarity to previous products or systems whose experience could predict hazards.

Fault Tree Analysis

Fault Tree Analysis finds its best application in complex situations because of the systematic way that various factors can be presented. It is, in effect, a model to which probability data can be applied in logical sequences.* Broadly, the method may be described as follows:

1. The undesirable event, or fault, whose possibility or probability is to be determined is selected. This event may be inadvertent or unauthorized launch of a missile, failure of an aircraft in flight, ignition of an ordnance device, injury to personnel, or any similar mishap.

2. System requirements, function, design, environment, and other factors are reviewed to determine conditions, events, and failures that could contribute to an occurrence of the undesired event.

---

*Ibid., pp. 238-239.

3. A tree is prepared diagramming contributory events and failures to show systematically their relation to each other and to the undesirable event being investigated. The process begins with the events that could directly cause the undesirable event (first level). As the procedure goes back step-by-step, combinations of events and failures that could bring about the end result are added. The diagrams so prepared are called <u>fault trees</u>.

4. The circumstances under which each of the events in the fault tree could occur are determined. Each component of the subsystem capable of producing an event is examined as to how its failure would contribute to a determined mishap. Other conditions or personnel actions that could have adverse effects are also included.

5. Suitable mathematical expressions representing the fault tree entries are developed using Boolean algebra. When more than one event on a chart can contribute to the same effect, the chart and the Boolean expression indicate whether the input events must all act in combination (AND in relationship) to produce the effect or whether they may act singly (OR in relationship). The mathematical expression of the AND/OR relationships for the tree is then simplified as much as possible.

6. The probability of failure of each component or of the occurrence of each condition or listed event is determined. These probabilities may be from failure rates obtained by past experience, vendors' test data, comparison with similar equipment, events, or conditions, or experimental data obtained specifically for the system.

7. These probabilities are then entered into the simplified Boolean expressions. The probability of occurrence of the undesirable event being investigated is then determined by calculation.

8. Other fallouts from use of the trees can be: determination of the most critical and probable sequence of events that could produce the undesirable event, identification of the most important affecting factors, single-point failure possibilities, and discovery of any sensitive elements whose improvement could reduce the possibility or probability of a mishap.

Certain assumptions and stipulations must be made concerning the characteristics of the components, conditions, actions, and events. These assumptions and stipulations regarding the components, action, events, etc., do apply, but they may not necessarily always apply in the stated fashion in the real world.

1. Components, subsystems, and similar items can have only two conditional modes: they can either operate successfully or fail. The formality of the system does not permit partially successful operations.

2. Basic failures are independent of each other.

3. Each item has a constant failure rate that conforms to an exponential distribution.

Reliability and Quality Assurance

The NASA Reliability and Quality Assurance publication* precisely defines reliability but not quality assurance. NASA defines reliability as: "A characteristic of a system, or any element thereof, expressed as a probability that it will perform its required functions under defined conditions at designated times for specified operating periods."

Quality Assurance is ensuring that a high-quality output is produced by the manufacturing and maintenance processes. It requires thorough planning and effective management of the whole Reliability and Quality Assurance effort and is concerned with inspecting and testing of all

---

*Reliability and Quality Assurance, Reliability Program Provisions for Aeronautical and Space System Contractors. Appendix C-2.

materials, parts, and assemblies received from suppliers. A contractor is responsible for the produce he furnishes a customer including all the items that he obtains from subcontractors and vendors.

The Quality Assurance effort may be divided into various phases: receipt of supplies to be processed, workmanship during the process, inspection of completed components, and inspection and testing of assemblies. Initial assurance that the items furnished by suppliers meet prescribed requirements (design and performance) can be undertaken at either the suppliers' plants, the receiving plant, or both. Tests or series of assurance tests are conducted to determine that the items supplied meet quality requirements. These tests are statistically designed with specific confidence levels to demonstrate reliability and quality.

Failure Mode, Effect, and Analysis*

Study of a system and the working interrelationships of its elements should include determining ways in which failures can occur (failure modes), effects of each potential failure on the system element in which it occurs and on other system elements, and the probable overall consequences (criticality) of each failure mode on the success of the system's mission. Criticalities are usually assigned by categories, each category being defined in terms of a specified degree of loss of mission objectives or degradation of crew safety.

---

*Ibid.

E. ELEMENTS OF A SYSTEMS SAFETY PROGRAM

Basic Elements

In order for a program manager to have maximum awareness of the risks he is assuming, there are certain safety tasks that must be accomplished and working relationships established to formalize a systems safety effort into a discipline. The NASA Systems Safety Manual* describes these tasks and working relationships in terms of nine elements in a systems safety program:

1. Planning

2. Organization

3. Contracting

4. Interface and coordination

5. Criteria

6. Analysis

7. Reporting

8. Evaluation

9. Data retention

These nine elements from the manual will be briefly discussed in the following pages in order to provide a framework for this report.

1. Planning

Planning consists of a review of pertinent historical safety data from similar systems, a review of hardware requirements and concepts, a

---
*NASA Safety Manual, Vol. 3, System Safety, 1970.

review of the system objectives, a planning of safety activities, and a preliminary hazard analysis to identify potentially hazardous systems in order to develop initial safety requirements and criteria. During this part of the program, system safety goals and objectives are established, and it is essential that the planning be flexible enough to meet changing needs.

NASA requires that the hardware system being developed be made as safe as feasible through the identification and control of hazards, but goes one step further by introducing the concepts of risk and risk assumption. NASA recognizes this concept of risk as shown in the statement below:

> The tasks that should be accomplished . . . to formalize the system safety effort into a discipline, to the end that the program manager will have maximum visibility into the risks he is assuming.

> The desired results from system safety activities are the minimizing of risks to the maximum practical extent and the application of the knowledge of these risks to management decisions.

> The product of system safety activities is the identification and evaluation of the risks encountered during the life cycle of the system and the utilization of this information by the appropriate levels of management.

2. Organization

After the planning phase is over, it is essential that an organization be set up to accomplish the tasks in the plan. The major safety tasks are broken down into subtasks, and responsibilities are assigned to various groups to accomplish them. The size and complexity of these

tasks and the safety organization are determined by the size and complexity of the system.

3. Contracting

In the Systems Safety program contracting has two forms: the safety effort may be contracted out as a special package or it may be set up as part of the total systems procurement package. The requirements being contracted out must be carefully prepared so that the contractor clearly understands what he is expected to accomplish.

4. Interface and Coordination

The effectiveness of a functional systems safety effort is determined by the quantity and quality of the output and the development of the output is dependent upon the interfaces established. Therefore, working interfaces should be established at the earliest possible time in the system development and, as each interface is established, the safety manager in a program should strive to reach a maximum data exchange with his counterparts. These may be located in:

    a. Safety Engineering

    b. Safety Reliability and Quality

    c. Safety Configuration Management

    d. Safety Manufacturing

    e. Safety Systems Test

    f. Safety Operations

    g. Safety Program Management

5. Criteria

Criteria are generated from the results of safety analysis and from experience gained from other programs using similar systems. These criteria are the "basic safety" which should be readily identifiable when necessary.

6. Analysis

System Safety Analyses are performed for the purpose of identifying hazards and establishing risk levels. Hazards are measured in four categories:

  a. Negligible - will not result in personal injury or systems damage.

  b. Marginal - can be counteracted or controlled without injury to personnel or system loss.

  c. Critical - will cause personnel injury or major system damage, or will require immediate corrective action to avoid personnel or system damage.

  d. Catastrophic - will cause death or severe injury to personnel or system loss.

These Safety Analyses perform five basic functions:

  a. Provide foundation for the development of safety criteria and requirements

  b. Determine whether and how the safety criteria and requirements provided to engineering have been included in the design

  c. Determine whether the safety criteria and requirements created for that design have provided adequate safety for the system

  d. Provide part of the means for meeting preestablished safety goals

  e. Provide means of demonstrating that safety goals have been met

7. Reporting

In setting up a Systems Safety program, the hazard identification/ hazard resolution should be defined in the various safety plans or contracts. Such definition simplifies and organizes the reporting aspects which, in turn, maximize the safety achieved in a systems safety program. In addition to the general types of reporting which consist of hazard identification and resolution, a Safety Analysis Report (SAR) which serves as a total record of the risks assumed in order to complete each mission is also prepared.

8. Evaluation

In order to assure that the safety goals sought are being met and that planned tasks are being accomplished, the safety program should be evaluated at various intervals during the program. Other purposes of evaluation should be:

    a. Assuring that the safety was properly structured

    b. Assuring good access to both the system data and proper management reporting level

    c. Assuring an output resulting from the Systems Safety effort

    d. Assuring that effective use is being made of safety output
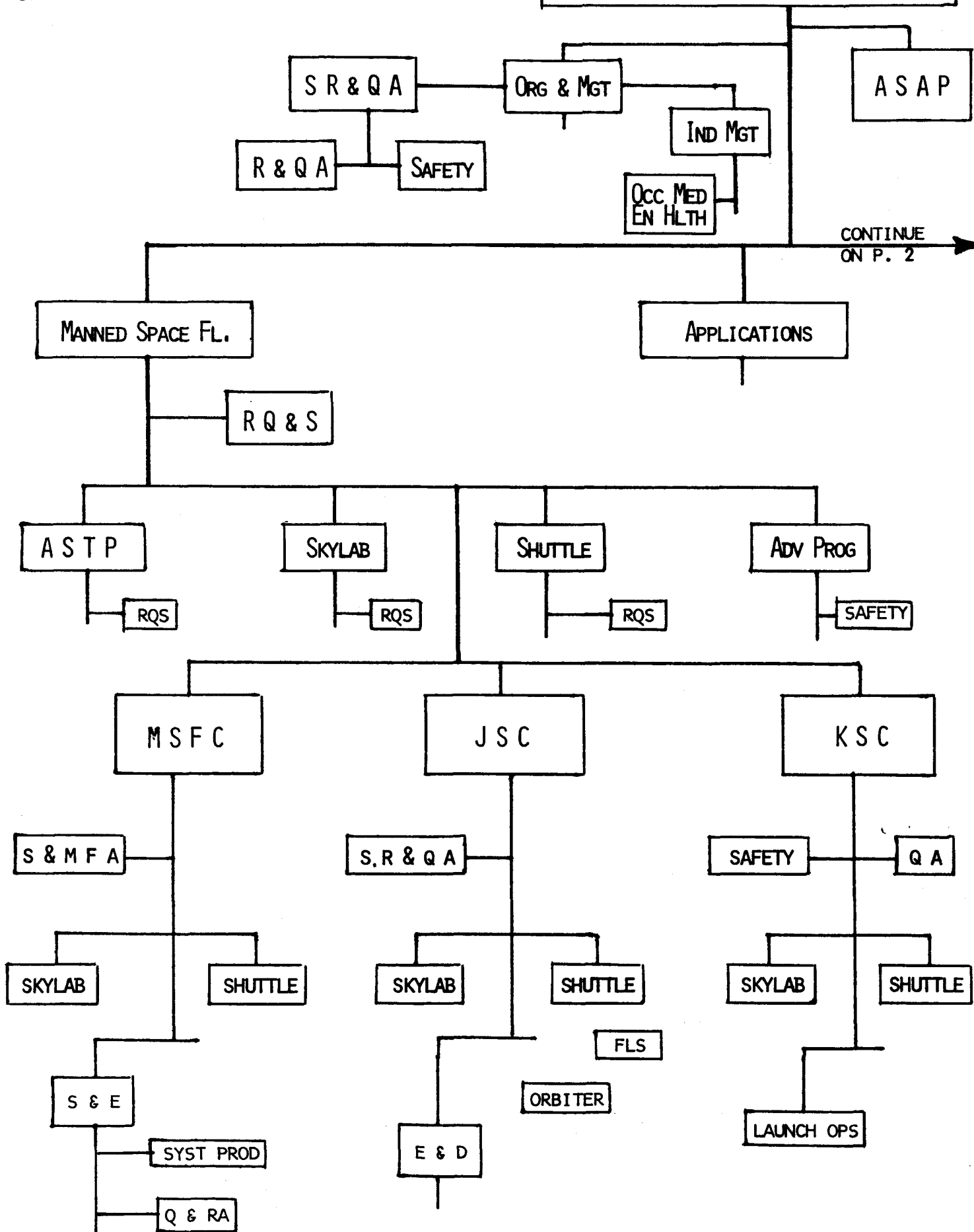
9. Data Retention

As a result of the previous elements of the Systems Safety program, there will be an extensive amount of systems safety data which will be accumulated. Among these are:

    a. Criteria requirements

    b. Safety study reports

    c.   Progress and activity reports

    d.   Safety analysis reports

    e.   Hazard reports

    f.   Accident reports

    g.   Other analyses

These items are valuable safety data that may have application to other systems presently being developed or to be developed in the future and, therefore, should be documented for retention as they are prepared.

- 122 -

NASA ADMINISTRATOR

SR&QA

ORG & MGT

IND MGT

OCC MED EN HLTH

ASAP

R&QA — SAFETY

MANNED SPACE FL.

APPLICATIONS

RQ&S

ASTP — RQS

SKYLAB — RQS

SHUTTLE — RQS

ADV PROG — SAFETY

MSFC

JSC

KSC

S & M F A

S.R & Q A

SAFETY — Q A

SKYLAB SHUTTLE

SKYLAB SHUTTLE

SKYLAB SHUTTLE

FLS

S & E

ORBITER

LAUNCH OPS

SYST PROD

E & D

Q & RA

MANAGEMENT of SAFETY at NASA

SKELETON of ORGANIZATION

NOTE: ONLY OFFICES REFERRED TO IN REPORT BY
SYRACUSE UNIVERSITY STUDY GROUP ARE SHOWN.